Algebraic aspects of the Number Field Sieve

Daniele Taufer

Advised by Prof. Dr. Hendrik Willem Lenstra

Universiteit Leiden

Universität Duisburg Essen

ALGANT Master's Thesis - June 24, 2016

To Hendrik and Jan,
for what I learned from them
and the way they thrilled me.

Contents

Introduction

The *Number Field Sieve* is an algorithm for factoring large integers. A first version of this algorithm was proposed in 1988 by John Pollard and was aimed to factor integers of the form $r^e - s$ where $r, |s|$ are small positive integers and e is a large one. As an instance, it is efficient in factoring Mersenne numbers ($M_n = 2^n - 1$) and Fermat numbers ($F_n = 2^{2^n} + 1$).

A later version of this algorithm for factoring any odd integer which is a not power of some prime was developed by J.P. Buhler, H.W. Lenstra and Carl Pomerance in 1993 (see [LL93]) and it is the one we will refer to in this work. A heuristic computation shows that the complexity for factoring an integer N is of the form

$$\exp\left((c + o(1))(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}\right) \quad \text{for } N \to \infty$$

and this makes the *Number Field Sieve* the most efficient classical algorithm known for factoring large integers.

From a theoretical point of view this algorithm presents some problems, which are nowadays still not solved; in this work we address one of these issues and we solve it modulo the following hypothesis.

Let $g \in \mathbb{Q}[X]$ be a monic rational polynomial with positive degree and discriminant $\Delta(g) \neq 0$; define $F := \mathbb{Q}[X]/g\mathbb{Q}[X] = \mathbb{Q}[\omega]$ where $\omega := (X \bmod g) \in F$ and $F_p := \mathbb{Q}_p \otimes_{\mathbb{Q}} F$. Let also $J \subseteq F^*$ be the subgroup generated by all elements of the form $(a - \omega)/(b - \omega)$, where a, b are integers larger than every real zero of g, and for a prime number p let $J_p \subseteq \mathbb{Q}_p[\omega]^*$ be the subgroup generated by all elements of the form $(a - \omega)/(b - \omega)$, where $a, b \in \mathbb{Z}_p$ satisfy $g(a) \neq 0$ and $g(b) \neq 0$.

Hypothesis (H.W. Lenstra)**.** *With the notation introduced above, an invertible element $\beta \in F^*$ belongs to J if and only if the following two conditions are satisfied:*

(i) $\varphi(\beta) > 0$ for every ring morphism $\varphi : F \to \mathbb{R}$.

(ii) for every prime p the image of β under $F^* \hookrightarrow F_p^*$ belongs to J_p.

Let us now call N the integer we want to factor. We assume N to be odd and divisible by at least two distinct primes. This is a reasonable assumption, because if N was a prime there would be nothing to factor, and this can be checked in polynomial time by making use of the AKS primality test (see [AKS02]); if $N > 2$ was even, we already know one of its proper factors (namely 2); finally, if N was the power of some natural number, we can quickly figure it out by checking for every $b \in \{2, \ldots, \lfloor \log_2(N) \rfloor\}$ if $N^{\frac{1}{b}}$ is an integer.

The *Number Field Sieve* makes use of a positive integer $d \in \mathbb{Z}_{>0}$, an integer $m \in \mathbb{Z}$ and a monic degree d polynomial $h(X) = \sum_{i=0}^{d} c_i X^i \in \mathbb{Z}[X]$ satisfying

$$h(m) \equiv 0 \bmod N, \qquad h(m) \neq 0, \qquad \gcd(h'(m), N) = 1, \qquad \Delta(h) \neq 0. \tag{$*$}$$

Let $E = \mathbb{Q}[X]/h\mathbb{Q}[X] = \mathbb{Q}[\gamma]$, and denote by C the integral closure of $\mathbb{Z}$ in E. The algorithm determines many triplets (Z, ϵ, e) where $Z \subseteq \mathbb{Z} \times \mathbb{Z}$ is a finite set of coprime pairs, $\epsilon \in E$ and $e \in \mathbb{Z}$, such that

$$\forall\ (a,b) \in Z : \gcd(a + bm, N) = 1, \qquad \prod_{(a,b)\in Z} (a + b\gamma) = \epsilon^2, \qquad \prod_{(a,b)\in Z} (a + bm) = e^2 \qquad (**)$$

and satisfying some inequalities that we will not examine here for simplicity. Consider now the ring morphism

$$\begin{aligned} \underline{\Psi}' : \mathbb{Z}[\gamma] &\to \mathbb{Z}/N\mathbb{Z} \\ \gamma &\mapsto (m \bmod N) \end{aligned}$$

which extends uniquely to a ring morphism $\underline{\Psi} : C \to \mathbb{Z}/N\mathbb{Z}$ as we will prove in the first chapter. If we apply this $\underline{\Psi}$ to a triplet with the properties $(**)$ described above, we get

$$\underline{\Psi}(\epsilon)^2 = (e \bmod N)^2 \in \mathbb{Z}/N\mathbb{Z} \quad \text{that is} \quad N \mid ([\underline{\Psi}(\epsilon)] - e)([\underline{\Psi}(\epsilon)] + e) \text{ in } \mathbb{Z}$$

where we denote $[x] \in \mathbb{Z}$ any integer representative of $x \in \mathbb{Z}/N\mathbb{Z}$. If N does not divide any of the two above factors, then $\gcd([\underline{\Psi}(\epsilon)] - e, N)$ will be a proper factor of N.

What the *Number Field Sieve* does at this point is to compute $\gcd([\underline{\Psi}(\epsilon)] - e, N)$ for a triplet generated as before, and if it is trivial (i.e. 1 or N) another triplet (Z, ϵ, e) is tried. One can reasonably wonder if there are particular starting conditions in terms of N and the elements satisfying conditions $(*)$ constructed by the *Number Field Sieve* for which this algorithm has no chances to end with a proper factor of N. The main theorem of our work is aimed to prove that, assuming the above hypothesis, this never happens even if we work with the extra condition $b = -1$.

Theorem. *Let N be an odd positive integer with at least two different prime factors and let $m \in \mathbb{Z}$, $d \in \mathbb{Z}_{>0}$ and $h(X) \in \mathbb{Z}[X]$ a monic degree d polynomial satisfying the conditions $(*)$. Then, if Lenstra's Hypothesis is true, there is a finite set of integers $S \subseteq \mathbb{Z}$, an element $\epsilon \in E$ and an integer $e \in \mathbb{Z}$ such that conditions $(**)$ hold for the set $Z := S \times \{-1\}$ and $\gcd([\underline{\Psi}(\epsilon)] - e, N) \notin \{1, N\}$.*

In order to prove the above theorem, we make use of some algebraic results that don't involve any hypothesis and which are therefore of independent interest from a theoretical point of view. We develop them in the first two chapters, which are kept logically independent of each other, and they will be used together with the Lenstra's Hypothesis in the last chapter to prove the result.

In Chapter 1 we give the general setting of our work and we prove that the above mentioned ring morphism $\underline{\Psi}$ can really be defined in a unique way from the given morphism $\underline{\Psi}'$ on $\mathbb{Z}[\gamma]$. This will follow from the main theorem of this chapter, which is the following.

Theorem. *Let R be a commutative ring, $R' \subseteq R$ a subring that is integrally closed in R and $h(X) \in R'[X]$ a monic polynomial. Let also $S := R[X]/hR[X] = R[\gamma]$ where $\gamma := (X \bmod h) \in S$ and C be the integral closure of R' in S. Then*

$$h'(\gamma) \cdot C \subseteq R'[\gamma].$$

In Chapter 2 we take F to be a product of number fields (i.e. a finite étale algebra over $\mathbb{Q}$), we prove that for every rational prime p the F_p previously defined are products of complete fields $F_{\mathfrak{p}}$ and we identify F^* as a subgroup of $\prod_{p\leq\infty} F_p^*$. Under this identification we can state the main theorem of the chapter, which is the following.

Theorem. *Let F be a finite étale algebra over $\mathbb{Q}$ and S a finite set of places of $\mathbb{Q}$ containing ∞. For any coset $U \subseteq \prod_{p\in S} F_p^*$ of any open subgroup of $\prod_{p\in S} F_p^*$ in the product topology, we have*

$$F^* \cap \left(U \times \prod_{p\notin S} \Big(\prod_{\substack{\mathfrak{p}|p \\ F_{\mathfrak{p}}=\mathbb{Q}_p}} F_{\mathfrak{p}}^* \times \prod_{\substack{\mathfrak{p}|p \\ F_{\mathfrak{p}}\neq\mathbb{Q}_p}} \mathcal{O}_{F_{\mathfrak{p}}}^* \Big) \right) \neq \emptyset.$$

The proof of this theorem, which fills the rest of this chapter, will make use of the ideles and their relation with the ray class group. In particular, we will make use of the fact that the degree one primes not dividing a given cycle generate the ray class group of that cycle.

In Chapter 3 we prove the theorem stated above on the lack of algebraic obstructions for the *Number Field Sieve* to end up with a proper factor of a given integer N. After a precise presentation of what we want to prove, the Lenstra's Hypothesis is stated and some properties of the groups involved (in particular the J_p's) are discussed. Afterwards, we give an interpretation of the non-triviality of the gcd involved in the statement in terms of finding an element with some algebraic properties. We make then use of the Hypothesis to shift the problem in the setting described in the previous chapter, where the existence of such an element will follow by applying the main result of Chapter 2.

In the Appendix some examples of practical (positive) tests of the Hypothesis are given. This does not affect the work and is proposing to see what the algebraic conditions of the Hypothesis turn out to be in some concrete case. It is likewise aimed to show how this assumption is "widely true" in the easy cases; this fact may give to the reader the feeling that something really evil should happen if a polynomial for which the Hypothesis does not hold can, one day, be exhibited.

Chapter 1

Preliminaries

1.1 The setting

Let N be an odd positive integer divisible by at least two distinct positive prime numbers. Suppose we are given an integer $m \in \mathbb{Z}$, a positive integer $d \in \mathbb{Z}_{>0}$ and a monic polynomial $h(X) = \sum_{i=0}^{d} h_i X^i \in \mathbb{Z}[X]$ of degree d (i.e. $h_d = 1$) satisfying the following conditions:

$$\begin{aligned} (i)\ & h(m) \equiv 0 \bmod N \\ (ii)\ & h(m) \neq 0 \\ (iii)\ & \gcd(h'(m), N) = 1 \\ (iv)\ & \Delta(h) \neq 0 \end{aligned} \tag{1.1}$$

where $\Delta(h)$ is the discriminant of h. We define $f(X) := (X - m) \cdot h(X)$ and

$$F := \mathbb{Q}[X]/f\mathbb{Q}[X] = \mathbb{Q}[\alpha] \text{ where } \alpha := (X \bmod f) \in F.$$

As we did for α, we can define $\gamma := (X \bmod h) \in \mathbb{Q}[X]/h\mathbb{Q}[X]$, so

$$E := \mathbb{Q}[X]/h\mathbb{Q}[X] = \mathbb{Q}[\gamma].$$

Since $h(m) \neq 0$ by condition (ii) in 1.1, we have $\gcd(X - m, h(X)) = 1$ in $\mathbb{Q}[X]$ so the Chinese Remainder Theorem gives us an explicit relation between F and E, which is given by the projections, which is

$$\begin{aligned} F = \mathbb{Q}[\alpha] &\xrightarrow{\sim} \mathbb{Q} \times E \\ \mathbb{Q} \ni q &\mapsto (q, q) \\ \alpha &\mapsto (m, \gamma). \end{aligned} \tag{1.2}$$

In the following we will identify F with $\mathbb{Q} \times E$ via the above isomorphism. It is convenient to give the following definition.

Definition 1.1.1 (finite étale algebra)**.** Let K be a field. A K-algebra L is said to be a *finite étale algebra over* K if it is isomorphic to a finite product of finite and separable field extensions of K.

With the above definition E needs not to be a field, h not being necessarily irreducible, but it is a finite étale algebra over $\mathbb{Q}$; in fact, by (iv) of our assumpions 1.1 we know that h has no multiple roots, then if $h = h_1 \cdots h_r \in \mathbb{Q}[X]$ is its factorization into irreducible polynomials, the h_i's are all different and the Chinese Remainder Theorem gives us:

$$E = \mathbb{Q}[X]/(h_1 \cdots h_r)\mathbb{Q}[X] \simeq H_1 \times \cdots \times H_r$$

where $H_i := \mathbb{Q}[X]/h_i\mathbb{Q}[X]$ are all finite separable extensions of $\mathbb{Q}$. Clearly also F is a finite étale algebra over $\mathbb{Q}$, being isomorphic to $\mathbb{Q} \times E$ as in 1.2.

We want to restrict the $\mathbb{Q}$-algebra isomorphism 1.2 to an isomorphism of the integral closures of $\mathbb{Z}$, and this follows as a particular case of the following lemma. We will denote for brevity $\mathrm{Ic}_R(F)$ the integral closure of a commutative ring R in an R-algebra F.

Lemma 1.1.2. *Let R be a commutative ring and $F_1, \ldots, F_n$ any R-algebras. Then:*

$$\mathrm{Ic}_R(F_1 \times \cdots \times F_n) = \mathrm{Ic}_R(F_1) \times \cdots \times \mathrm{Ic}_R(F_n).$$

Proof. $\subseteq$) Let $\underline{b} = (b_1, \ldots, b_n) \in \mathrm{Ic}_R(F_1 \times \cdots \times F_n)$, then there exists $p(X) \in R[X]$ monic such that $p(\underline{b}) = 0$, which means (since the operations are componentwise) that $p(b_i) = 0$ for every index i, so $b_i \in \mathrm{Ic}_R(F_i)$ for every i.
$\supseteq$) Let b_1 (resp. $b_2, \ldots, b_n$) be in $\mathrm{Ic}_R(F_1)$ $\big($resp. $\mathrm{Ic}_R(F_2), \ldots, \mathrm{Ic}_R(F_n)\big)$; this means that for every i there exists a monic polynomial $p_i(X) \in R[X]$ such that $p_i(b_i) = 0$. Then the polynomial $p(X) = p_1(X) \cdots p_n(X) \in R[X]$ is still monic and vanishes in $\underline{b} = (b_1, \ldots, b_n)$, i.e. $\underline{b} \in \mathrm{Ic}_R(F_1 \times \cdots \times F_n)$. $\square$

The above lemma tells us in particular that the ring of integers of a finite étale algebra is the product of the rings of integers of its components.

Let from now on B and C be the integral closures of $\mathbb{Z}$ in F and E respectively. By Lemma 1.1.2 we know that the isomorphism 1.2 restricts to a $\mathbb{Z}$-algebras isomorphism:

$$\begin{aligned} B &\simeq \mathbb{Z} \times C \\ \alpha &\longleftrightarrow (m, \gamma). \end{aligned}$$

In the following we will identify B with $\mathbb{Z} \times C$ under this isomorphism.

1.2 A property of the integral closures

In this section we prove some general results of commutative algebra that we will eventually use for the proof of the following theorem.

Theorem 1.2.1. *Let R be a commutative ring, $R' \subseteq R$ a subring that is integrally closed in R and $h(X) \in R'[X]$ a monic polynomial. Let also $S := R[X]/hR[X] = R[\gamma]$ where $\gamma := (X \ mod\ h) \in S$ and $C := \mathrm{Ic}_{R'}(S)$. Then*

$$h'(\gamma) \cdot C \subseteq R'[\gamma].$$

Let R be a commutative ring; we will denote as usual

$$R(\!(X)\!) := \{\sum_{i \geq n_0} r_i X^i \mid n_0 \in \mathbb{Z},\ r_i \in R\}$$

the ring of the Laurent series with coefficients in R. The first lemma shows that the trace morphism extends naturally to the Laurent series.

Lemma 1.2.2. *Let R be a commutative ring and S an R-algebra that is free of finite rank as an R-module. Then $S(\!(X)\!)$ is a free $R(\!(X)\!)$-module of the same rank and there is a unique $R(\!(X)\!)$-linear morphism extending $\mathrm{Tr}_{S|R}$ to $S(\!(X)\!)$, namely $\mathrm{Tr}_{S(\!(X)\!)|R(\!(X)\!)}$. Moreover, for every $\sum_{i\geq n_0} t_iX^i \in S(\!(X)\!)$, this morphism satisfies*

$$\mathrm{Tr}_{S(\!(X)\!)|R(\!(X)\!)}\big(\sum_{i\geq n_0} t_iX^i\big) = \sum_{i\geq n_0} \mathrm{Tr}_{S|R}(t_i)X^i.$$

Proof. We have the isomorphism of R-algebras

$$\begin{aligned} R(\!(X)\!) \otimes_R S &\xrightarrow{\sim} S(\!(X)\!) \\ \sum_{i\geq n_0} r_iX^i \otimes s &\mapsto \sum_{i\geq n_0} (s\cdot r_i)X^i \end{aligned}$$

Thus, if $d = [S : R]$ and $s_1, \ldots, s_d$ is an R-basis of S, then $1\otimes s_1, \ldots, 1\otimes s_d$ is an $R(\!(X)\!)$-basis of $R(\!(X)\!) \otimes_R S \simeq S(\!(X)\!)$. Therefore the trace morphism

$$\begin{aligned} \mathrm{Tr}_{S(\!(X)\!)|R(\!(X)\!)} = \mathrm{id}_{R(\!(X)\!)} \otimes \mathrm{Tr}_{S|R} : R(\!(X)\!) \otimes_R S &\to R(\!(X)\!) \\ \sum_{i\geq n_0} r_iX^i \otimes s &\mapsto \sum_{i\geq n_0} r_iX^i \otimes \mathrm{Tr}_{S|R}(s) \end{aligned}$$

extends $\mathrm{Tr}_{S|R}(s)$ from $1\otimes S \simeq S$. As for the uniqueness, let $\varphi : R(\!(X)\!)\otimes_R S \to R(\!(X)\!)\otimes_R S$ an $R(\!(X)\!)$-linear morphism that acts like $\mathrm{Tr}_{S|R}$ on $1\otimes_R S$. Then

$$\forall\ 0 \leq i \leq d : \varphi(1\otimes s_i) = 1\otimes \mathrm{Tr}_{S|R}(s_i) = \mathrm{Tr}_{S(\!(X)\!)|R(\!(X)\!)}(1\otimes s_i)$$

so $\varphi = \mathrm{Tr}_{S(\!(X)\!)|R(\!(X)\!)}$ since they are equal on an $R(\!(X)\!)$-basis of $S(\!(X)\!)$. Let now us define the map

$$\begin{aligned} \mathrm{Tr}' : S(\!(X)\!) &\to R(\!(X)\!) \\ \sum_{i\geq n_0} t_iX^i &\mapsto \sum_{i\geq n_0} \mathrm{Tr}_{S|R}(t_i)X^i. \end{aligned}$$

It respects the additive group structure since the trace $\mathrm{Tr}_{S|R}$ is linear and it also respects the multiplication by elements $\sum_{j\geq m_0} r_jX^j \in R(\!(X)\!)$ because

$$\begin{aligned} \mathrm{Tr}'\big((\sum_{j\geq m_0} r_jX^j)(\sum_{i\geq n_0} t_iX^i)\big) &= \mathrm{Tr}'\big(\sum_{l\geq n_0+m_0} (\sum_{j+i=l} r_jt_i)X^l\big) \\ &= \sum_{l\geq n_0+m_0} \mathrm{Tr}_{S|R}(\sum_{j+i=l} r_jt_i)X^l \\ &= \sum_{l\geq n_0+m_0} \big(\sum_{j+i=l} r_j\mathrm{Tr}_{S|R}(t_i)X^l\big) \\ &= \big(\sum_{j\geq m_0} r_jX^j\big)\cdot \mathrm{Tr}'\big(\sum_{i\geq n_0} t_iX^i\big) \end{aligned}$$

where the third equality holds because $\mathrm{Tr}_{S|R}$ is R-linear. Since Tr' patently extends $\mathrm{Tr}_{S|R}$, the uniqueness part of the above statement gives us $\mathrm{Tr}' = \mathrm{Tr}_{S(\!(X)\!)|R(\!(X)\!)}$, which is exactly what we wanted to prove. $\square$

In the following we will use the previous proposition with X^{-1} in the place of X, but clearly nothing changes. The second lemma gives us a very explicit relation between the coefficients of the minimal polynomial of an element and those of its inverse.

Lemma 1.2.3. *Let R be a commutative ring and S an R-algebra that is free of finite rank as an R-module; let also $s \in S^*$ be an invertible element and*

$$\chi_s(Y) = Y^d + a_{d-1}Y^{d-1} + \cdots + a_1 Y + a_0 \in R[X]$$

its characteristic polynomial. Then the characteristic polynomial of s^{-1} is

$$\chi_{s^{-1}}(Y) = Y^d + \frac{a_1}{a_0}Y^{d-1} + \cdots + \frac{a_{d-1}}{a_0}Y + \frac{1}{a_0}.$$

Proof. Let A be the matrix of the multiplication by s; since $a_0 = (-1)^d \cdot \det A$ and A is invertible, $\frac{1}{a_0} = a_0^{-1} \in R$ makes sense. Therefore we have

$$\begin{aligned} a_0 \cdot \chi_{s^{-1}}(Y) &= (-1)^d \cdot \det A \cdot \det(Y - A^{-1}) = (-1)^d \cdot \det(AY - 1) = Y^d \cdot \det(\frac{1}{Y} - A) \\ &= Y^d \cdot \chi_s(\frac{1}{Y}) \end{aligned}$$

and this is exactly what we wanted to prove. □

Now we specialize the setting to the case $S := R[X]/hR[X] = R[\gamma]$ as in Theorem 1.2.1. We know that S is a free R-module of rank $d := \deg(h)$ generated by $\{1, \gamma, \ldots, \gamma^{d-1}\}$, in fact there is the R-module isomorphism

$$\begin{aligned} R^d &\xrightarrow{\sim} S \\ (r_0, \ldots, r_{d-1}) &\mapsto \sum_{i=0}^{d-1} r_i \gamma^i. \end{aligned} \tag{1.3}$$

Since S is free of finite rank over R, we have the trace morphism $\mathrm{Tr}_{S|R} : S \to R$ and the last-projection morphism $\pi : S \to R$ sending $\sum_{i=0}^{d-1} r_i\gamma^i \mapsto r_{d-1}$, both belonging to $\mathrm{Hom}_R(S, R)$, as well as the projections on the coefficient of γ^i for every i. Every $\varphi \in \mathrm{Hom}_R(S, R)$ is determined by its images on the basis $\{1, \gamma, \ldots, \gamma^{d-1}\}$, hence there is a natural R-module isomorphism

$$\begin{aligned} \mathrm{Hom}_R(S, R) &\xrightarrow{\sim} R^d \\ \varphi &\mapsto (\varphi(\gamma^j))_{j=0,\ldots,d-1}. \end{aligned} \tag{1.4}$$

We can also see $\mathrm{Hom}_R(S, R)$ as an S-module, with the operation given by

$$\forall\ s \in S, \varphi \in \mathrm{Hom}_R(S, R) : s \star \varphi(x) := \varphi(s \cdot x)$$

The following lemma tells us that with this new module structure, $\mathrm{Hom}_R(S, R)$ is free of rank 1.

Lemma 1.2.4. *With the operation $\star$ as above, $\mathrm{Hom}_R(S, R)$ is a free S-module of rank 1, generated by the last projection π. In other words, S and $\mathrm{Hom}_R(S, R)$ are isomorphic as S-modules via*

$$\begin{aligned} S &\xrightarrow{\sim} \mathrm{Hom}_R(S, R) \\ s &\mapsto s \star \pi. \end{aligned}$$

Proof. The above map is patently a morphism of S-modules, so we just need to prove that it is bijective. It is in particolar a morphism of R-modules, so we may consider the R-linear map given by

$$R^d \xrightarrow{\sim} S \longrightarrow \mathrm{Hom}_R(S,R) \xrightarrow{\sim} R^d$$

$$(r_i)_{i=0,\dots,d-1} \longmapsto \sum_{i=0}^{d-1} r_i\gamma^i \longmapsto \sum_{i=0}^{d-1} \big((r_i\gamma^i)\star\pi\big) \longmapsto \left(\sum_{i=0}^{d-1} \pi(r_i\gamma^i\gamma^j)\right)_{j=0,\dots,d-1}$$

where the first and the last isomorphisms are given by 1.3 and 1.4 respectively. The matrix of this R-linear morphism can be easily computed on the standard basis $e_k := (\delta_{i,k})_{i=0,\dots,d-1}$ of R^d, and it is given by

$$\big(\pi(\gamma^{i+j})\big)_{\substack{0\le i\le d-1\\ 0\le j\le d-1}} = \begin{pmatrix} 0 & 0 & \dots & & 0 & 1 \\ 0 & \ddots & & 0 & 1 & * \\ \vdots & & 0 & 1 & * & \\ & 0 & 1 & * & & \vdots \\ 0 & 1 & * & & \ddots & * \\ 1 & * & & \dots & * & * \end{pmatrix}$$

where the $* \in R$ are elements that we are not interested in computing; this is because $i+j < d-1$ implies $\pi(\gamma^{i+j}) = 0$ while when $i+j = d-1$ we get $\pi(\gamma^{i+j}) = \pi(\gamma^{d-1}) = 1$. Then the composite morphism is invertible, so the middle one is. □

Note that the previous proof only depends on the fact that S is a free R-module generated by $1,\gamma,\dots,\gamma^{d-1}$. If we call $T = R'[X]/hR'[X] = R'[\gamma]$, which we can do since $h(X) \in R'[X]$ actually, it is still free on R' with the same basis $1,\gamma,\dots,\gamma^{d-1}$ then Lemma 1.2.4 gives us also an isomorphism of T-modules

$$\begin{aligned} T &\xrightarrow{\sim} \mathrm{Hom}_{R'}(T,R') \\ t &\mapsto t\star\pi. \end{aligned}$$

We have the natural inclusion

$$\begin{aligned} T = R'[\gamma] &\hookrightarrow R[\gamma] = S \\ \gamma^i &\mapsto \gamma^i \end{aligned}$$

given by the scalar extension ($S = R\otimes_{R'} T$) and

$$\begin{aligned} \mathrm{Hom}_{R'}(T,R') &\hookrightarrow \mathrm{Hom}_R(S,R) \\ (\gamma^i \mapsto r_i) &\mapsto (\gamma^i \mapsto r_i) \end{aligned}$$

given by sending an R'-linear map into the R-linear map that has the same image over the basis $1,\gamma,\dots,\gamma^{d-1}$. The above morphisms are clearly both R'-linear.

Lemma 1.2.5. *With the notation introduced above, the following*

$$\begin{tikzcd} S \arrow[r, "\sim"] & \mathrm{Hom}_R(S,R) \\ T \arrow[r, "\sim"] \arrow[u, hook] & \mathrm{Hom}_{R'}(T,R') \arrow[u, hook] \end{tikzcd}$$

is a commutative diagram of R'-modules.

Proof. All the maps involved are R'-linear, so it is sufficient to check that the two different routes act in the same way on the basis $1, \gamma, \dots, \gamma^{d-1}$, which is trivial since they both send $\gamma^i \in T$ into $\gamma^i \star \pi \in \mathrm{Hom}_R(S,R)$. □

We are now ready to prove the crucial propositions that we will use in the proof of Theorem 1.2.1. The argument we use follows an idea of Daniel J. Bernstein.

Proposition 1.2.6. *With the above notation, we have*

$$\frac{h'(X)}{h(X)} = \sum_{m\geq 0} \frac{\mathrm{Tr}_{S|R}(\gamma^m)}{X^{m+1}} \in R(\!(X^{-1})\!).$$

Proof. By Lemma 1.2.2 we have

$$\sum_{m\geq 0} \frac{\mathrm{Tr}_{S|R}(\gamma^m)}{X^{m+1}} = \sum_{m\geq 0} \frac{\mathrm{Tr}_{S(\!(X^{-1})\!)|R(\!(X^{-1})\!)}(\gamma^m)}{X^{m+1}} = \mathrm{Tr}_{S(\!(X^{-1})\!)|R(\!(X^{-1})\!)}\Big(\sum_{m\geq 0} \frac{\gamma^m}{X^{m+1}}\Big). \tag{1.5}$$

Note that $\sum_{m\geq 0} \frac{\gamma^m}{X^{m+1}}$ is invertible in $S(\!(X^{-1})\!)$, since

$$\sum_{m\geq 0} \frac{\gamma^m}{X^{m+1}} = \frac{1}{X}\sum_{m\geq 0} \big(\frac{\gamma}{X}\big)^m = X^{-1}\big(1-\frac{\gamma}{X}\big)^{-1} = (X-\gamma)^{-1}. \tag{1.6}$$

By the Hamilton-Cayley Theorem we know that the characteristic polynomial of γ is $\chi_\gamma(Y) := \det(Y-\gamma) = h(Y)$. Then the minimal polynomial of $X-\gamma$ is

$$\chi_{(X-\gamma)}(Y) = \det\big(Y-(X-\gamma)\big) = \det\Big((-1)\big((X-Y)-\gamma\big)\Big) = (-1)^d h(X-Y).$$

Therefore

$$\begin{aligned} \chi_{(X-\gamma)}(Y) &= (-1)^d h(X-Y) \\ &= (-1)^d h(X) + (-1)^{d+1} h'(X)Y + (\text{higher degree terms in } Y). \end{aligned}$$

The constant term of $\chi_{(X-\gamma)}(Y)$ is the norm of an invertible element of $S(\!(X^{-1})\!)$, so is invertible itself in $R(\!(X^{-1})\!)$, then $\frac{1}{h(X)}$ makes sense in $R(\!(X^{-1})\!)$. It is also well-known that the coefficient of the term Y^{d-1} in $\chi_{(X-\gamma)^{-1}}(Y)$ is $-\mathrm{Tr}_{S(\!(X^{-1})\!)|R(\!(X^{-1})\!)}\big((X-\gamma)^{-1}\big)$, and we know it by Lemma 1.2.3 as a quotient between the two coefficients of the lower degree terms in $\chi_{(X-\gamma)}(Y)$, namely

$$\mathrm{Tr}_{S(\!(X^{-1})\!)|R(\!(X^{-1})\!)}\big((X-\gamma)^{-1}\big) = -\frac{(-1)^{\deg h+1}h'(X)}{(-1)^{\deg h}h(X)} = \frac{h'(X)}{h(X)} \tag{1.7}$$

By equations 1.5, 1.6 and 1.7 the result follows. □

Proposition 1.2.7. *With the operation $\star$ as above, we have*

$$\mathrm{Tr}_{S|R} = h'(\gamma) \star \pi \in \mathrm{Hom}_R(S, R).$$

Proof. Let $k \in \mathbb{Z}_{\geq 0}$ be a fixed non-negative integer; by Proposition 1.2.6 we have

$$X^k h'(X) = X^k h(X) \sum_{m \geq 0} \frac{\mathrm{Tr}_{S|R}(\gamma^m)}{X^{m+1}} = h(X)g(X) + z(X) \tag{1.8}$$

where

$$g(X) := X^k \sum_{m=0}^{k-1} \frac{\mathrm{Tr}_{S|R}(\gamma^m)}{X^{m+1}} \in R[X]$$
$$z(X) := h(X)\Big(X^k \sum_{m \geq k} \frac{\mathrm{Tr}_{S|R}(\gamma^m)}{X^{m+1}}\Big) \in R(\!(X^{-1})\!).$$

Observe that also $z(X)$ has to be a polynomial, because by 1.8 it is the difference of the two polynomials

$$z(X) = X^k h'(X) - h(X)g(X) \in R[X] \tag{1.9}$$

The degree of $z(X)$ is at most $d-1$ because of its definition, and since $h(X)$ is monic the coefficient of X^{d-1} in $z(X)$ is $\mathrm{Tr}_{S|R}(\gamma^k)$. Since the equation 1.9 is a polynomial relation, we can substitute γ for X and in view of $h(\gamma) = 0$ it becomes

$$z(\gamma) = \gamma^k h'(\gamma).$$

Taking in the above equation the projection π on the coefficient of γ^{d-1}, we finally obtain

$$\mathrm{Tr}_{S|R}(\gamma^k) = \pi\big(\gamma^k h'(\gamma)\big) = h'(\gamma) \star \pi(\gamma^k).$$

The above equation holds for every possible starting choice of $k \in \mathbb{Z}_{\geq 0}$, so $\mathrm{Tr}_{S|R}$ and $h'(\gamma) \star \pi$ are equal on an R-basis of S, then they are equal in $\mathrm{Hom}_R(S, R)$. □

Before proving the main theorem of this section, we need a last technical lemma on the trace morphism.

Lemma 1.2.8. *Let R be a commutative ring and $R' \subseteq R$ a subring. Let also S be an R-algebra that is free of finite rank as an R-module. Then for every $c \in S$ integral over R', the coefficients of its characteristic polynomial $\chi_c(X) \in R[X]$ are integral over R' and the trace morphism $\mathrm{Tr}_{S|R} : S \to R$ restricts to a morphism*

$$\mathrm{Tr}_{S|R} : \mathrm{Ic}_{R'}(S) \to \mathrm{Ic}_{R'}(R)$$

between the integral closures of R'.

Proof. Let $c \in S$ be integral over R' and $g(X) \in R'[X]$ be a monic polynomial such that $g(c) = 0$, so $(X - c) \mid g(X)$ in $S[X]$. Let also $\chi_c(X) \in R[X]$ be the characteristic polynomial of c. We know that

$$\chi_c(X) = \det(X - c) = \mathrm{N}_{S[X]|R[X]}(X - c)$$

and by the multiplicativity of the norm we also have

$$(X-c) \mid g(X) \Rightarrow \mathrm{N}_{S[X]|R[X]}(X-c) \mid \mathrm{N}_{S[X]|R[X]}\big(g(X)\big) = g(X)^{[S:R]} =: l(X).$$

For any monic polynomial $p(X) \in R[X]$ a ring $K \supseteq R$ such that $p(X)$ splits into linear factors in $K[X]$ can always be constructed in a finite number of steps, as follows. Consider the ring $K' := R[Y]/p(Y)R[Y] = R[\beta]$ where $\beta = (Y \bmod p)$; the ring $K'[X]$ contains a linear factor of $p(X)$, namely $(X-\beta)$, so $p(X) = \widetilde{p}(X) \cdot (X-\beta)$ for some $\widetilde{p}(X) \in K'[X]$ with degree lower than $\deg(p(X))$. We iterate this construction on $\widetilde{p}(X)$ in place of $p(X)$ until we end up with a ring $K[X]$ where $p(X)$ splits into linear factors.

Consider then such a ring $K \supseteq R$ where χ_c splits in linear factors, i.e.

$$\chi_c(X) = \prod_{i=1}^{t}(X-\beta_i) \in K[X].$$

Observe that every $\beta_i \in K$ is integral over R', because it is a zero of $\chi_c(X)$ and therefore of the monic polynomial $l(X) \in R'[X]$, which $\chi_c(X)$ divides. The coefficients of χ_c are explicit polynomial expressions of the β_i's (Vieta formulas) and the integral elements form a ring, then we conclude that every coefficient of χ_c is in $\mathrm{Ic}_{R'}(R)$, so in particular the coefficient of X^{t-1} $\big($which is $-\mathrm{Tr}_{S|R}(c)\big)$ is integral over R'. □

Now we can finally prove Theorem 1.2.1.

Proof of Theorem 1.2.1. We first prove that we have the equality of sets

$$\{x \in S \mid h'(\gamma) \cdot x \in T\} = \{x \in S \mid \mathrm{Tr}_{S|R}(x \cdot T) \subseteq R'\}.$$

$\subseteq$) Let $x \in S$ such that $h'(\gamma) \cdot x \in T$; by Proposition 1.2.7 we have

$$\mathrm{Tr}_{S|R}(x \cdot T) = \pi\big(h'(\gamma) \cdot x \cdot T\big) \subseteq R'$$

where the inclusion holds because $h'(\gamma) \cdot x \cdot T \subseteq T = R'[\gamma]$, so in particular the coefficient of γ^{d-1} is in R'.

$\supseteq$) Let $x \in S$ such that $\mathrm{Tr}_{S|R}(x \cdot \beta) \in R'$ for every $\beta \in T$; we want to prove that the coefficients of γ^i in $h'(\gamma) \cdot x$ are in R' for every i. Let $\pi_j = (\sum_{i=0}^{d-1} r_i\gamma^i \mapsto r_j) : S \to R$ be the projections on these coefficients. Since any projection of $\mathrm{Hom}_R(S,R)$ comes actually from the corresponding projection of $\mathrm{Hom}_{R'}(T,R')$, Lemma 1.2.4 tells us that there are $t_1, \ldots, t_n \in T$ such that

$$t_j \star \pi = \pi_j \in \mathrm{Hom}_R(S,R).$$

Therefore, using again Proposition 1.2.7, the coefficient of γ^j in $h'(\gamma) \cdot x$ is

$$\pi_j\big(h'(\gamma) \cdot x\big) = \pi\big(h'(\gamma) \cdot x \cdot t_j\big) = \mathrm{Tr}_{S|R}(x \cdot t_j) \in R'$$

because $\mathrm{Tr}_{S|R}(x \cdot \beta) \in R'$ for every $\beta \in T$. This proves that all the projections of $h'(\gamma) \cdot x$ (which in principle are in R) belong actually to R', i.e. $h'(\gamma) \cdot x \in R'[\gamma] = T$.

Given the above equality of sets, Theorem 1.2.1 follows immediately observing that the right hand side contains C in view of Lemma 1.2.8 and because we assumed $R' \subseteq R$ to be integrally closed, i.e. $\mathrm{Ic}_{R'}(R) = R'$. □

1.3 The factoring map

In this section we want to construct a group morphism that will lead us to a non-trivial factor of N in the last section. Consider the ring morphisms given by

$$\begin{aligned}\psi_1 : \mathbb{Z} &\to \mathbb{Z}/N\mathbb{Z}\\ n &\mapsto (n \bmod N)\end{aligned}$$

and

$$\begin{aligned}\overline{\psi_2} : \mathbb{Z}[\gamma] &\to \mathbb{Z}/N\mathbb{Z}\\ n &\mapsto (n \bmod N)\\ \gamma &\mapsto (m \bmod N).\end{aligned}$$

Observe that $\overline{\psi_2}$ is really a ring morphism because of the condition (i) in 1.1. We would like to extend it to a ring morphism from C, and the following lemma tells us that there is a unique way how to do it.

Lemma 1.3.1. *Let S and A be commutative rings, $R \subseteq S$ a subring and $f : R \to A$ a ring morphism. If there is an element $r \in R$ such that $f(r) \in A^*$ and $R \supseteq rS$, then there exists a unique ring morphism $g : S \to A$ extending f, given by*

$$g(s) := f(sr) \cdot f(r)^{-1} \ \forall\ s \in S.$$

Proof. If such an element r exists, for every $s \in S$ we have $sr \in R$ so any such ring morphism g exending f has to satisfy

$$g(s)f(r) = g(s)g(r) = g(sr) = f(sr) \quad \forall s \in S.$$

Thus, after multiplying by the inverse of $f(r)$, we see that the only possible value of $g(s)$ is $f(sr) \cdot f(r)^{-1}$. As for the existence, it is easy to check that the g map defined above is a ring morphism: it is clearly additive and sends 1_R into 1_A, while the following

$$g(s_1s_2) = f(s_1s_2r) \cdot f(r)^{-1} = f(s_1rs_2r) \cdot f(r)^{-2} = f(s_1r) \cdot f(s_2r) \cdot f(r)^{-2} = g(s_1) \cdot g(s_2)$$

proves that it also respects products. □

By Theorem 1.2.1 applied with $R' = \mathbb{Z}$ and $R = \mathbb{Q}$, we know that if C is the integral closure of $\mathbb{Z}$ in $E = \mathbb{Q}[X]/h\mathbb{Q}[X] = \mathbb{Q}[\gamma]$, then

$$h'(\gamma) \cdot C \subseteq \mathbb{Z}[\gamma].$$

Note also that $\overline{\psi_2}\big(h'(\gamma)\big) = h'(m) \in (\mathbb{Z}/N\mathbb{Z})^*$ because of the assumption (iii) in 1.1. Thus, we can apply Lemma 1.3.1 with $R = \mathbb{Z}[\gamma]$, $S = C$, $A = \mathbb{Z}/N\mathbb{Z}$, $r = h'(\gamma) \in R$ and $f = \overline{\psi_2}$, obtaining the unique extended ring morphism

$$\begin{aligned}\psi_2 : C &\to \mathbb{Z}/N\mathbb{Z}\\ c &\mapsto \Big(\overline{\psi_2}(h'(\gamma) \cdot c) \cdot \big(h'(m)\big)^{-1} \bmod N\Big)\end{aligned}$$

Finally we can define the map of our interest, which is

$$\begin{aligned}\Psi : B \simeq \mathbb{Z} \times C &\to \mathbb{Z}/N\mathbb{Z}\\ (n, c) &\mapsto \big(\psi_1(n) - \psi_2(c) \bmod N\big).\end{aligned}$$

Note that Ψ is patently a surjective additive group morphism, but it is not a ring morphism (e.g. it sends $B \ni 1 \mapsto 0 \in \mathbb{Z}/N\mathbb{Z}$).

Chapter 2

Degree one primes and ideles

2.1 The Degree One Theorem

In this section we present a purely algebraic theorem that will be the key tool for proving the main result of the following chapter.

Let $F_1, \dots, F_r$ be number fields and $F = F_1 \times \cdots \times F_r$ be a finite étale algebra over $\mathbb{Q}$ as defined in section 1.1. We know that for every $R_1, \dots, R_n$ commutative rings we have

$$\mathrm{Spec}(\prod_{i=1}^{n} R_i) = \bigsqcup_{i=1}^{n} \mathrm{Spec} R_i$$

so we may talk about finite places of a product meaning the union of the finite places of all the coordinates.

For every prime $p \in \mathbb{Z}$ we define

$$F_p := \mathbb{Q}_p \otimes_{\mathbb{Q}} F.$$

With this notation, we have

$$F_p \simeq (\mathbb{Q}_p \otimes_{\mathbb{Q}} F_1) \times \cdots \times (\mathbb{Q}_p \otimes_{\mathbb{Q}} F_r) = (F_1)_p \times \cdots \times (F_r)_p$$

where $(F_i)_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} F_i$ are not fields in general. Anyway, since for every i the field F_i is a finite (separable) extension of $\mathbb{Q}$, then $F_i = \mathbb{Q}[X]/f_i\mathbb{Q}[X]$ for some separable $f_i \in \mathbb{Q}[X]$, so if $f_i = f_{i1} \cdots f_{ih}$ is the factorization of f in $\mathbb{Q}_p[X]$, then $(F_i)_p = \prod_{j=1}^{h} \mathbb{Q}_p[X]/f_{ij}\mathbb{Q}_p[X]$.

Theorem 2.1.1. *Let $|\cdot|$ be an absolute value on a field F and $\widehat{F}$ the corresponding completion of F. Let also $E = F(u)$ where u is algebraic over F with minimum polynomial $f(X)$ over F and let $f_1(X), \dots, f_h(X)$ be the distinct monic irreducible factors of $f(X)$ in $\widehat{F}[X]$. Then there are exactly h extensions of $|\cdot|$ to absolute values on E. The corresponding completions are isomorphic to the fields $\widehat{F}[X]/f_j(X)\widehat{F}[X]$, $1 \leq j \leq h$.*

Proof. See chapter 9, [Jac12]. □

The previous theorem with $F = \mathbb{Q}$, together with $|\cdot| = |\cdot|_p$ and $E = F_i$, allows us to write every $(F_i)_p$ as a product of finite field extensions of $\mathbb{Q}_p$, namely the completions of F_i with respect to finite places $\mathfrak{p}$ over p, i.e.

$$(F_i)_p = \prod_{\mathfrak{p}|p} (F_i)_{\mathfrak{p}}.$$

Therefore we can write

$$F_p = \prod_{\mathfrak{p}|p} F_{\mathfrak{p}}$$

where the $F_{\mathfrak{p}}$ are all finite extensions of $\mathbb{Q}_p$. Since (chapter 2, [CF67]) any finite extension of a completely valued non-archimedean field is itself complete and non-archimedean with respect to the unique extended valuation, then $F_{\mathfrak{p}}$ are complete and non-archimedean fields for every finite place $\mathfrak{p}$ of F. We denote as usual $\mathcal{O}_L$ the ring of integers of a non-archimedean field L.

Similarly to the finite case, we can define

$$F_\infty := \mathbb{R} \otimes_{\mathbb{Q}} F \simeq \prod_{i=i}^{r} (F_i)_\infty$$

and the above arguments with $\mathbb{R}$ in place of $\mathbb{Q}_p$ tell us that also F_∞ is a product of some copies of $\mathbb{R}$ and some copies of $\mathbb{C}$, corresponding respectively to the real and the complex places of F. If $\mathfrak{p}$ is an infinite place of some F_i we will write $\mathfrak{p}|\infty$, and with this notation we have

$$F_\infty = \prod_{\mathfrak{p}|\infty} F_{\mathfrak{p}}$$

where the fields $F_{\mathfrak{p}}$ are all $\mathbb{R}$ or $\mathbb{C}$.

For every place $p \leq \infty$ of $\mathbb{Q}$ we know by the above definitions that F is a subring of $F_p = \prod_{\mathfrak{p}|p} F_{\mathfrak{p}}$ (because $\mathbb{Q}_p$ is faithfully flat over $\mathbb{Q}$), so we have a natural injective ring morphism

$$F \hookrightarrow \prod_{p \leq \infty} F_p = \prod_{p \leq \infty} \Big(\prod_{\mathfrak{p}|p} F_{\mathfrak{p}}\Big).$$

In the following we will always see this injection as an identification. The main theorem of this section can be finally stated; the meaning of its name will be better understood in its proof, at the last section of this chapter.

Theorem 2.1.2 (Degree One Theorem)**.** *Let F be a finite étale algebra over $\mathbb{Q}$ and S a finite set of places of $\mathbb{Q}$ containing ∞. For any coset $U \subseteq \prod_{p \in S} F_p^*$ of any open subgroup of $\prod_{p \in S} F_p^*$ in the product topology, we have*

$$F^* \cap \Bigg(U \times \prod_{p \notin S} \Big(\prod_{\substack{\mathfrak{p}|p \\ F_{\mathfrak{p}} = \mathbb{Q}_p}} F_{\mathfrak{p}}^* \times \prod_{\substack{\mathfrak{p}|p \\ F_{\mathfrak{p}} \neq \mathbb{Q}_p}} \mathcal{O}_{F_{\mathfrak{p}}}^* \Big)\Bigg) \neq \emptyset.$$

2.2 The Idele Group and the Ray Class Group

Here we want to recall some definitions and results that really come from general algebraic number theory. We begin with an important definition.

Definition 2.2.1 (restricted product)**.** Let I be a set and for every $i \in I$ let X_i be a topological space. Suppose that for almost every $i \in I$ an open $O_i \subseteq X_i$ is given. We define the *restricted product of the $\{X_i\}_{i \in S}$ with respect to the O_i's* to be

$$\prod_{i \in I}{}' X_i := \Big\{ (x_i)_{i \in I} \in \prod_{i \in I} X_i \mid x_i \in O_i \text{ for almost every } i \in I \Big\}.$$

The restricted product is a topological space by taking as a base of the topology the sets of the form $\prod_{i\in I} U_i \subseteq \prod'_{i\in I} X_i$ where U_i is an open subset of X_i for every $i \in I$ and $U_i = O_i$ for almost all $i \in I$.

Let us denote with $\mathfrak{P}_F$ the set of places of a number field F, and for every $\mathfrak{p} \in \mathfrak{P}_F$ let $F_\mathfrak{p}$ be the completion of F with respect to a valuation representing the place $\mathfrak{p}$, as we did in section 2.1. We know that we can identify finite places $\mathfrak{p}$ of F with the elements of $\bigsqcup_{p<\infty} \mathrm{Spec} F_p$ and we will write $\mathfrak{p}|p$ if $\mathfrak{p}$ lies above $p\mathbb{Z}$; we will also write $\mathfrak{p}|\infty$ if the place is infinite (complex or real). Since there are only finitely many infinite places, we can give the following definition.

Definition 2.2.2 (idele group)**.** Let F be a number field. We define the *idele group* of F to be the restricted product

$$\mathcal{I}_F := \prod_{\mathfrak{p}\in\mathfrak{P}_F}' F_\mathfrak{p}^*$$

where the restriction is with respect to $\{\mathcal{O}_{F_\mathfrak{p}}^*\}_{\mathfrak{p}\in\mathrm{Spec}F}$.

We may identify F^* as a subgroup of its idele group, via the natural inclusion map

$$\begin{aligned} F^* &\hookrightarrow \mathcal{I}_F \\ x &\mapsto (x)_{\mathfrak{p}\in\mathfrak{P}_F} \end{aligned}$$

which is well-defined according to the following lemma.

Lemma 2.2.3. *Let F be a number field and $\alpha \in F^*$ a non-zero element of F. Then there are only finitely many inequivalent valuations $|\cdot|$ of F for which*

$$|\alpha| \neq 1.$$

Proof. See chapter 2, [CF67]. □

It is well-known that $F_\mathfrak{p}^*$ is a topological group for every finite place $\mathfrak{p} \in \mathrm{Spec}\mathcal{O}_F$. We want here to recall a couple of results about these objects.

Lemma 2.2.4. *Let G be a topological group and H a subgroup of G. Then H is open if and only if it contains a non-empty open subset $U \subseteq G$.*

Proof. If H is open, $U = H$ works. On the other side, let $U \subseteq H$ an open subset of G and let $u \in U$. Then for every $h \in H$ the set $V_h := (hu^{-1}) \cdot U$ is an open of G contained in H and containing h; thus, H is open. □

Lemma 2.2.5. *Let G_1, G_2 be topological groups and H a subgroup of $G_1 \times G_2$. Then H is open if and only if it contains $A \times B \subseteq G_1 \times G_2$ with A (resp. B) an open subgroup of G_1 (resp. G_2).*

Proof. If $H \supseteq A \times B$ with A and B open (and non-empty) in the respective spaces, then H contain a non-empty open set of $G_1 \times G_2$ so by Lemma 2.2.4 it is open. On the other hand, since H is an open subgroup it contains $\widetilde{A} \times \widetilde{B}$ where $\widetilde{A}$ (resp. $\widetilde{B}$) is an open subset of G_1 (resp. G_2) containing 1, because these sets form a base of the neighbourhoods of $(1,1)$ in the product topology. Then

$$H \supseteq \langle \widetilde{A} \times \widetilde{B} \rangle = \langle \widetilde{A} \rangle \times \langle \widetilde{B} \rangle =: A \times B$$

where A (resp. B) is an open subgroup of G_1 (resp. G_2) by using again Lemma 2.2.4. □

For every finite place $\mathfrak{p} \in \mathrm{Spec}\mathcal{O}_F$, let $\hat{\mathfrak{p}}$ be the maximal ideal of $\mathcal{O}_{F_\mathfrak{p}}$; we define

$$U_\mathfrak{p}^{(n)} := \begin{cases} \mathcal{O}_{F_\mathfrak{p}}^* & \text{if } n = 0 \\ 1 + \hat{\mathfrak{p}}^n & \text{if } n > 0 \end{cases}$$

while for every infinite place $\mathfrak{p}|\infty$ we define

$$U_\mathfrak{p}^{(n)} := \begin{cases} F_\mathfrak{p}^* & \text{if } n = 0 \\ (F_\mathfrak{p}^*)^2 & \text{if } n = 1 \text{ and } \mathfrak{p} \text{ is a real place.} \end{cases}$$

We have the following characterization of the open subgroups of $F_\mathfrak{p}^*$.

Proposition 2.2.6. *Let F a number field, $\mathfrak{p} \in \mathfrak{P}_F$ one of its places and $H \subseteq F_\mathfrak{p}^*$ a subgroup. Then H is open if and only $U_\mathfrak{p}^{(n)} \subseteq H$ for some $n \in \mathbb{Z}_{\geq 0}$ for which $U_\mathfrak{p}^{(n)}$ is defined.*

Proof. When $\mathfrak{p}$ is infinite it is trivial: the only open multiplicative subgroups of $\mathbb{R}^*$ are $\mathbb{R}^*$ itself and $(\mathbb{R}^*)^2 = \mathbb{R}_{>0}$, while the only open multiplicative subgroup of $\mathbb{C}^*$ is the whole $\mathbb{C}^*$. Let us now assume $\mathfrak{p}$ to be a finite place; since $(1+\hat{\mathfrak{p}}^n)_{n\geq 1}$ is a base for the neighbourhoods of 1, if H is open it contains $1 + \hat{\mathfrak{p}}^n$ for every $n \geq n_0$ (for some $n_0 \in \mathbb{Z}_{\geq 1}$). On the other hand, if H contains any open set $1 + \hat{\mathfrak{p}}^n$, by Lemma 2.2.5 it is open. □

Definition 2.2.7 (cycle)**.** Let F be a number field. A *cycle* (or *modulus*) of F is a function $n : \mathfrak{P}_F \to \mathbb{Z}_{\geq 0}$ satisfying the following three conditions.

(i) $n(\mathfrak{p}) = 0$ for all but finitely many $\mathfrak{p} \in \mathfrak{P}_F$.
(ii) $n(\mathfrak{p}) = 0$ if $\mathfrak{p}$ is a complex place.
(iii) $n(\mathfrak{p}) \in \{0, 1\}$ if $\mathfrak{p}$ is a real place.

We will usually write a cycle as $\mathfrak{f} = \prod_{\mathfrak{p}\in\mathfrak{P}_F} \mathfrak{p}^{n(\mathfrak{p})}$.

For any cycle $\mathfrak{f}$, we may define

$$W_\mathfrak{f} := \prod_{\mathfrak{p}\in\mathfrak{P}_F} U_\mathfrak{p}^{(n(\mathfrak{p}))}.$$

We can therefore characterize the open subgroups of $\mathcal{I}_F$ as follows.

Proposition 2.2.8. *Let F be a number field and $H \subseteq \mathcal{I}_F$ a subgroup. Then H is open if and only if there exists a cycle $\mathfrak{f}$ such that $W_\mathfrak{f} \subseteq H$.*

Proof. It follows immediately from the definition of open sets in the restricted products jointly with Proposition 2.2.6. □

Definition 2.2.9 (ray class group)**.** Let $\mathfrak{f} = \prod_{\mathfrak{p}\in\mathfrak{P}_F} \mathfrak{p}^{n(\mathfrak{p})}$ a cycle of the number field F. We say that an element $\alpha \in F^*$ satisfies

$$\alpha \equiv 1 \bmod^* \mathfrak{f}$$

if $\alpha \in U_\mathfrak{p}^{(n(\mathfrak{p}))}$ whenever $n(\mathfrak{p}) > 0$. We define the *ray class group* of $\mathfrak{f}$ to be

$$\mathrm{Cl}_\mathfrak{f} := \langle \mathfrak{p} \in \mathrm{Maxspec}\mathcal{O}_F \mid n(\mathfrak{p}) = 0\rangle / \langle \alpha\mathcal{O}_F \mid \alpha \in F^*,\ \alpha \equiv 1 \bmod^* \mathfrak{f}\rangle.$$

Let us denote as usual the inertia degree of a prime $\mathfrak{p}$ by $\deg \mathfrak{p} := [\mathcal{O}_F/\mathfrak{p} : \mathbb{F}_p]$. As for the standard class group case, $\mathrm{Cl}_{\mathfrak{f}}$ is generated by the classes of the primes of degree one, eventually omitting a finite number of them.

Theorem 2.2.10. *Let $\mathfrak{f}$ be a cycle of the number field F and T a finite set of primes of F containing the primes dividing $\mathfrak{f}$. Then the ray class group $\mathrm{Cl}_{\mathfrak{f}}$ satisfies*

$$\mathrm{Cl}_{\mathfrak{f}} = \langle [\mathfrak{p}] \mid \deg \mathfrak{p} = 1, \mathfrak{p} \notin T \rangle.$$

Proof. See Theorem 2 in [LS91]. □

2.3 Reduction to the number field case

In this section we prove that Theorem 2.1.2 is really equivalent to the same theorem where F is required to be a number field. Clearly if it holds for every finite étale algebra over $\mathbb{Q}$, it holds for every number field. The following proposition shows that the converse is also true.

Proposition 2.3.1. *Assume that Theorem 2.1.2 holds whenever F is a number field. Then it holds also as stated for any arbitrary finite étale algebra F over $\mathbb{Q}$.*

Proof. Let F be a finite étale algebra over $\mathbb{Q}$, so $F = F_1 \times \cdots \times F_r$ where every F_i is a number field. Let S a finite set of places of $\mathbb{Q}$ containing ∞ and $U = U_1 \times \cdots \times U_r$ be the coset of the open subgroup A' represented by the element $\lambda = (\lambda_1, \ldots, \lambda_r) \in \prod_{p \in S} F_p^*$, i.e. $U = \lambda A'$. By Lemma 2.2.5 we know that $A' \supseteq A = A_1 \times \cdots \times A_r$ with A_i an open subgroup of $\prod_{p \in S} (F_i)_p^*$ for every $1 \leq i \leq r$. Therefore if we define

$$U_i := \lambda_i A_i$$

these are all cosets of open subgroups of $\prod_{p \in S} (F_i)_p^*$. Thus, we can apply for every $1 \leq i \leq r$ the number field version of Theorem 2.1.2 with F_i and U_i as defined above, together with the given S, finding for every i an element $\beta_i \in (F_i)^*$ such that

$$\beta_i \in U_i \times \prod_{p \notin S} \Big(\prod_{\substack{\mathfrak{p} \mid p \\ (F_i)_{\mathfrak{p}} = \mathbb{Q}_p}} (F_i)_{\mathfrak{p}}^* \times \prod_{\substack{\mathfrak{p} \mid p \\ (F_i)_{\mathfrak{p}} \neq \mathbb{Q}_p}} \mathcal{O}_{(F_i)_{\mathfrak{p}}}^* \Big).$$

The element

$$\beta := (\beta_i)_{i=1,\ldots,n} \in \prod_{i=1}^{r} (F_i)^* = F^*$$

is in the desired intersection, in fact $\prod_{i=1}^{r} U_i = \lambda A \subseteq \lambda A' = U$ so

$$\beta \in \prod_{i=1}^{r} \left(U_i \times \prod_{p \notin S} \Big(\prod_{\substack{\mathfrak{p} \mid p \\ (F_i)_{\mathfrak{p}} = \mathbb{Q}_p}} (F_i)_{\mathfrak{p}}^* \times \prod_{\substack{\mathfrak{p} \mid p \\ (F_i)_{\mathfrak{p}} \neq \mathbb{Q}_p}} \mathcal{O}_{(F_i)_{\mathfrak{p}}}^* \Big) \right) \subseteq U \times \prod_{p \notin S} \Big(\prod_{\substack{\mathfrak{p} \mid p \\ F_{\mathfrak{p}} = \mathbb{Q}_p}} F_{\mathfrak{p}}^* \times \prod_{\substack{\mathfrak{p} \mid p \\ F_{\mathfrak{p}} \neq \mathbb{Q}_p}} \mathcal{O}_{F_{\mathfrak{p}}}^* \Big).$$

Thus, if Theorem 2.1.2 holds for every number field, it is also true for arbitrary finite étale algebras over $\mathbb{Q}$. □

Here we just want to point out that every β_i constructed above belongs to F_i, which is a number field. This implies, by Lemma 2.2.3, that

$$\beta_i \in U_i \times \prod_{p \notin S}{}' \Big(\prod_{\substack{\mathfrak{p}|p \\ (F_i)_\mathfrak{p} = \mathbb{Q}_p}} (F_i)_\mathfrak{p}^* \times \prod_{\substack{\mathfrak{p}|p \\ (F_i)_\mathfrak{p} \neq \mathbb{Q}_p}} \mathcal{O}_{(F_i)_\mathfrak{p}}^* \Big).$$

where the restriction is with respect to $\prod_{\mathfrak{p}|p} \mathcal{O}_{(F_i)_\mathfrak{p}}^*$ for p varying among the rational primes not in S, so the final β actually lies in

$$\beta \in U \times \prod_{p \notin S}{}' \Big(\prod_{\substack{\mathfrak{p}|p \\ F_\mathfrak{p} = \mathbb{Q}_p}} F_\mathfrak{p}^* \times \prod_{\substack{\mathfrak{p}|p \\ F_\mathfrak{p} \neq \mathbb{Q}_p}} \mathcal{O}_{F_\mathfrak{p}}^* \Big).$$

where the restricted product is with respect to $\prod_{\mathfrak{p}|p} \mathcal{O}_{F_\mathfrak{p}}^*$ for p varying among the rational primes not in S.

2.4 Proof of the Theorem

Here we prove Theorem 2.1.2 when F is a number field, which suffices by Proposition 2.3.1. Besides F, we are given a finite set S of places of $\mathbb{Q}$ containing ∞ and a coset U of some open subgroup A of $\prod_{p \in S} F_p^*$. Let us define

$$S_F := \{\mathfrak{p} \in \mathfrak{P}_F \mid \exists\, p \in S : \mathfrak{p}|p\}.$$

Since $\prod_{p \in S} F_p^*$ has the product topology (it is a finite product), Proposition 2.2.6 tells us that $A \supseteq \prod_{\mathfrak{p} \in S_F} U_\mathfrak{p}^{(n(\mathfrak{p}))} =: U'$ for some cycle $n(\cdot)$ of F represented by

$$\mathfrak{f} := \prod_{\mathfrak{p} \in S_F} \mathfrak{p}^{n(\mathfrak{p})}.$$

Here we may assume, up to restricting U', that for every finite place $\mathfrak{p} \in S_F$ we have $n(\mathfrak{p}) > 0$. This cycle defines, as we saw in the previous section, an open subgroup of $\mathcal{I}_F$ given by

$$W_\mathfrak{f} = \Big(\prod_{\mathfrak{p} \in S_F} U_\mathfrak{p}^{(n(\mathfrak{p}))} \Big) \times \Big(\prod_{\mathfrak{p} \notin S_F} \mathcal{O}_{F_\mathfrak{p}}^* \Big).$$

Consider then the group morphism given by

$$\Phi : F^* \hookrightarrow \mathcal{I}_F \twoheadrightarrow \mathcal{I}_F / W_\mathfrak{f}.$$

Recall that for every finite place $\mathfrak{p}$ we have the following group isomorphism

$$\begin{aligned} F_\mathfrak{p}^* / \mathcal{O}_{F_\mathfrak{p}}^* &\xrightarrow{\sim} \mathbb{Z} \\ \pi_\mathfrak{p}^n &\mapsto n \end{aligned}$$

where $\pi_{\mathfrak{p}}$ is a uniformizer of $\mathcal{O}_{F_{\mathfrak{p}}}$. Since any element of the idele group is in the unit group of the corresponding ring of integers for almost every coordinate by the very definition of restricted product, we have

$$\mathcal{I}_F/W_{\mathfrak{f}} \simeq \Big(\prod_{\mathfrak{p}\in S_F} F_{\mathfrak{p}}^*/U_{\mathfrak{p}}^{(n(\mathfrak{p}))}\Big) \times \Big(\bigoplus_{\substack{\mathfrak{p}\notin S_F\\ F_{\mathfrak{p}}=\mathbb{Q}_p}} \mathbb{Z}\Big) \times \Big(\bigoplus_{\substack{\mathfrak{p}\notin S_F\\ F_{\mathfrak{p}}\neq\mathbb{Q}_p}} \mathbb{Z}\Big).$$

Let us for brevity denote by $*$ be the coordinates of an element in $\bigoplus_{\substack{\mathfrak{p}\notin S_F\\ F_{\mathfrak{p}}=\mathbb{Q}_p}} \mathbb{Z}$ that we are not interested in considering explicitly.

Lemma 2.4.1. *In the above setting, assume that*

$$\forall\ (x_{\mathfrak{p}})_{\mathfrak{p}\in S_F} \in \prod_{\mathfrak{p}\in S_F} F_{\mathfrak{p}}^*/U_{\mathfrak{p}}^{(n(\mathfrak{p}))} \quad \exists\ y\in F^* : \Phi(y) = (z_{\mathfrak{p}})_{\mathfrak{p}\in\mathfrak{P}_F}$$
$$\text{where } z_{\mathfrak{p}} := \begin{cases} x_{\mathfrak{p}} & \text{if } \mathfrak{p}\in S_F \\ * & \text{if } \mathfrak{p}\notin S_F \text{ and } F_{\mathfrak{p}}=\mathbb{Q}_p \\ 0 & \text{if } \mathfrak{p}\notin S_F \text{ and } F_{\mathfrak{p}}\neq\mathbb{Q}_p. \end{cases} \tag{i}$$

Then there exists an element $y\in F^*$ such that

$$y \in U \times \prod_{p\notin S}\Big(\prod_{\substack{\mathfrak{p}|p\\ F_{\mathfrak{p}}=\mathbb{Q}_p}} F_{\mathfrak{p}}^* \times \prod_{\substack{\mathfrak{p}|p\\ F_{\mathfrak{p}}\neq\mathbb{Q}_p}} \mathcal{O}_{F_{\mathfrak{p}}}^*\Big).$$

Proof. Let U be the coset $x\cdot A \supseteq x\cdot U'$ for some $x=(x_{\mathfrak{p}})_{\mathfrak{p}\in S_F}\in\prod_{\mathfrak{p}\in S_F}F_{\mathfrak{p}}^*$; the $y\in F^*$ given by conditions (i), which is $(y_{\mathfrak{p}})_{\mathfrak{p}\in\mathfrak{P}_F}$ inside $\mathcal{I}_F$, satisfies

$$\begin{cases} \forall\ \mathfrak{p}\in S_F :\ y_{\mathfrak{p}} \in x_{\mathfrak{p}} U_{\mathfrak{p}}^{(n(\mathfrak{p}))} \\ \forall\ \mathfrak{p}\notin S_F, F_{\mathfrak{p}}\neq\mathbb{Q}_p :\ y_{\mathfrak{p}}\in\mathcal{O}_{F_{\mathfrak{p}}}^*. \end{cases}$$

The first line implies that $(y_{\mathfrak{p}})_{\mathfrak{p}\in S_F}\in x\cdot U'\subseteq U$ then, in view of the second line, we have $y\in U\times\prod_{p\notin S}\big(\prod_{\substack{\mathfrak{p}|p\\ F_{\mathfrak{p}}=\mathbb{Q}_p}} F_{\mathfrak{p}}^*\times\prod_{\substack{\mathfrak{p}|p\\ F_{\mathfrak{p}}\neq\mathbb{Q}_p}}\mathcal{O}_{F_{\mathfrak{p}}}^*\big)$ as required. □

We now prove that the condition (i) holds if another one does.

Lemma 2.4.2. *In the above setting, assume that*

$$\forall\ (w_{\mathfrak{p}})_{\substack{\mathfrak{p}\notin S_F\\ F_{\mathfrak{p}}\neq\mathbb{Q}_p}} \in \bigoplus_{\substack{\mathfrak{p}\notin S_F\\ F_{\mathfrak{p}}\neq\mathbb{Q}_p}} \mathbb{Z} \quad \exists\ v\in F^*\cap U' : \Phi(v) = (z_{\mathfrak{p}})_{\mathfrak{p}\in\mathfrak{P}_F}$$
$$\text{where } z_{\mathfrak{p}} := \begin{cases} 1 & \text{if } \mathfrak{p}\in S_F \\ * & \text{if } \mathfrak{p}\notin S_F \text{ and } F_{\mathfrak{p}}=\mathbb{Q}_p \\ w_{\mathfrak{p}} & \text{if } \mathfrak{p}\notin S_F \text{ and } F_{\mathfrak{p}}\neq\mathbb{Q}_p. \end{cases} \tag{ii}$$

Then the condition (i) of Lemma 2.4.1 holds.

Proof. Given any $x = (x_{\mathfrak{p}})_{\mathfrak{p}\in S_F} \in \prod_{\mathfrak{p}\in S_F} F_{\mathfrak{p}}^*/U_{\mathfrak{p}}^{(n(\mathfrak{p}))}$, we know that F^* is dense in $\prod_{\mathfrak{p}\in S_F} F_{\mathfrak{p}}^*$ (see chapter II, [CF67]) and that xU' is open, so we can find an element $y' \in F^* \cap xU'$. The image of such y' under Φ will be

$$\Phi(y') = (z_{\mathfrak{p}})_{\mathfrak{p}\in\mathfrak{P}_F} \text{ where } z_{\mathfrak{p}} = \begin{cases} x_{\mathfrak{p}} & \text{if } \mathfrak{p} \in S_F \\ * & \text{if } \mathfrak{p} \notin S_F \text{ and } F_{\mathfrak{p}} = \mathbb{Q}_p \\ -w_{\mathfrak{p}} & \text{if } \mathfrak{p} \notin S_F \text{ and } F_{\mathfrak{p}} \neq \mathbb{Q}_p \end{cases}$$

for some $w = (w_{\mathfrak{p}})_{\substack{\mathfrak{p}\notin S_F \\ F_{\mathfrak{p}}\neq\mathbb{Q}_p}} \in \bigoplus_{\substack{\mathfrak{p}\notin S_F \\ F_{\mathfrak{p}}\neq\mathbb{Q}_p}} \mathbb{Z}$. By applying the condition (ii) on this w we obtain an element $v \in F^*$, and the element $y := v \cdot y'$ satisfies condition (i) for the given x. □

Before proving Theorem 2.1.2, let us recall a well-known property of the finite field extensions $F_{\mathfrak{p}}$ of $\mathbb{Q}_p$.

Lemma 2.4.3. *Let F be a number field and $\mathfrak{p}|p$ a finite place of F, i.e. $\mathfrak{p} \in \mathrm{Spec}\mathcal{O}_F$. Then with the notation as above, we have $F_{\mathfrak{p}} = \mathbb{Q}_p$ if and only if $\deg \mathfrak{p} = 1$ and $\mathfrak{p}$ is an unramified prime.*

Proof. Since $F_{\mathfrak{p}}|\mathbb{Q}_p$ is finite, $\mathcal{O}_{f_{\mathfrak{p}}}$ is a DVR (see chapter 2, [CF67]), then there is a unique maximal ideal over $p\mathbb{Z}_p$, which is $\mathfrak{p}$. Hence the fundamental identity gives us

$$[F_{\mathfrak{p}} : \mathbb{Q}_p] = \sum_{\mathfrak{p}|p\mathbb{Z}_p} e(\mathfrak{p}|p\mathbb{Z}_p)f(\mathfrak{p}|p\mathbb{Z}_p) = e(\mathfrak{p}|p\mathbb{Z}_p)f(\mathfrak{p}|p\mathbb{Z}_p)$$

then the extension has degree one if and only if $f(\mathfrak{p}|p\mathbb{Z}_p) = \deg \mathfrak{p} = 1$ and $e(\mathfrak{p}|p\mathbb{Z}_p) = 1$ (i.e. $\mathfrak{p}$ is unramified). □

Now we can finally prove the main theorem of this chapter.

Proof of Theorem 2.1.2. If we prove that condition (ii) of Lemma 2.4.2 holds, by applying Lemma 2.4.2 and Lemma 2.4.1 we get the desired result.

For any given $w = (w_{\mathfrak{p}})_{\substack{\mathfrak{p}\notin S_F \\ F_{\mathfrak{p}}\neq\mathbb{Q}_p}} \in \bigoplus_{\substack{\mathfrak{p}\notin S_F \\ F_{\mathfrak{p}}\neq\mathbb{Q}_p}} \mathbb{Z}$ we can consider the ideal of $\mathcal{O}_F$ given by

$$\mathfrak{a}_w := \prod_{\substack{\mathfrak{p}\notin S_F \\ F_{\mathfrak{p}}\neq\mathbb{Q}_p}} \mathfrak{p}^{w_{\mathfrak{p}}} \in \mathrm{Cl}_{\mathfrak{f}}.$$

Let R be the finite set of primes of $\mathcal{O}_F$ that ramify, and set $T := R \cup S_F$; clearly T is still finite. By Theorem 2.2.10 there is an ideal

$$\mathfrak{a}_t = \prod_{\substack{\mathfrak{p}\in\mathrm{Cl}_{\mathfrak{f}} \\ \deg\mathfrak{p}=1 \\ \mathfrak{p}\notin T}} \mathfrak{p}^{t_{\mathfrak{p}}} \in \mathrm{Cl}_{\mathfrak{f}}$$

such that all but finitely many $t_{\mathfrak{p}}$ are zero and

$$[\mathfrak{a}_w] = [\mathfrak{a}_t] \in \mathrm{Cl}_{\mathfrak{f}}.$$

This means that there is a $v \in F^*$ satisfying $v \equiv 1 \bmod^* \mathfrak{f}$ such that

$$\mathfrak{a}_w = \mathfrak{a}_t \cdot (v) \Rightarrow (v) = \mathfrak{a}_w \cdot (\mathfrak{a}_t)^{-1}.$$

Observe that $v \equiv 1 \bmod^* \mathfrak{f}$ means by definition that $v \in F^* \cap U'$. Note also that by Lemma 2.4.3 the condition $(\deg \mathfrak{p} = 1 \wedge \mathfrak{p} \notin R)$ is equivalent to $F_\mathfrak{p} = \mathbb{Q}_p$. Thus, we have

$$\mathfrak{a}_t = \prod_{\substack{\mathfrak{p} \notin S_F \\ F_\mathfrak{p} = \mathbb{Q}_p}} \mathfrak{p}^{t_\mathfrak{p}} \in \mathrm{Cl}_\mathfrak{f}$$

for some $t = (t_\mathfrak{p})_{\substack{\mathfrak{p} \notin S_F \\ F_\mathfrak{p} = \mathbb{Q}_p}} \in \bigoplus_{\substack{\mathfrak{p} \notin S_F \\ F_\mathfrak{p} = \mathbb{Q}_p}} \mathbb{Z}$. Hence

$$\Phi(v) = (z_\mathfrak{p})_{\mathfrak{p} \in \mathfrak{P}_F} \text{ where } z_\mathfrak{p} = \begin{cases} \underline{1} & \text{if } \mathfrak{p} \in S_F \\ -t_\mathfrak{p} & \text{if } \mathfrak{p} \notin S_F \text{ and } F_\mathfrak{p} = \mathbb{Q}_p \\ w_\mathfrak{p} & \text{if } \mathfrak{p} \notin S_F \text{ and } F_\mathfrak{p} \neq \mathbb{Q}_p. \end{cases}$$

Then we found an element v satifying the condition (ii), completing the proof. $\square$

Chapter 3

The Number Field Sieve

3.1 The purpose

The *Number Field Sieve* is an algorithm used for factoring (large) integers, returning one of their proper factors. Let us call N the positive integer we want to factorize with this algorithm; for the reasons discussed in the introduction, we may assume N to be odd and with at least two different positive prime factors.

Given such an integer, the algorithm makes use of an integer $m \in \mathbb{Z}$, a positive integer $d \in \mathbb{Z}_{>0}$ and a monic degree d polynomial $h(X) = \sum_{i=0}^{d} h_i X^i \in \mathbb{Z}[X]$ satisfying the conditions 1.1 mentioned in the first section, which we recall here for convenience.

$$h(m) \equiv 0 \bmod N, \qquad h(m) \neq 0, \qquad \gcd\left(h'(m), N\right) = 1, \qquad \Delta(h) \neq 0. \tag{3.1}$$

Let also as in that section $f(X) := (X - m)h(X)$ and consider the two finite étale algebras over $\mathbb{Q}$ defined by $F := \mathbb{Q}[X]/f\mathbb{Q}[X] = \mathbb{Q}[\alpha]$ and $E := \mathbb{Q}[X]/h\mathbb{Q}[X] = \mathbb{Q}[\gamma]$. Define $w := \frac{\alpha - m - 1}{N}$ and let h_w be the minimal polynomial of w over $\mathbb{Q}$. Finally, let B and C be the integral closures of $\mathbb{Z}$ in F and E respectively; the simplified version of the algorithm determines (many) finite sets of integers $S \subseteq \mathbb{Z}$ and elements $\beta \in B$ satisfying the conditions

$$\begin{aligned} &(i)\ \forall\, a \in S : \gcd(a - m, N) = 1 \\ &(ii)\ \prod_{a \in S} (a - \alpha) = \beta^2. \end{aligned} \tag{3.2}$$

The factor of N computed by the *Number Field Sieve* from this set S is $\gcd([\Psi(\beta)], N)$ where $\Psi : B \to \mathbb{Z}/N\mathbb{Z}$ is the group morphism we constructed in section 1.3, and $[\Psi(\beta)]$ is meant to be one (any) integer representative of $\Psi(\beta) \in \mathbb{Z}/N\mathbb{Z}$. If this is a proper factor of N then the algorithm ends successfully, otherwise a different set S satisfying the conditions 3.2 is tried.

The purpose of this chapter is to prove that, if the Hypothesis 3.2.2 explained in the next chapter is true, there are no algebraic obstructions for the *Number Field Sieve* to end with a proper factor of N. This is formally expressed by the following theorem.

Theorem 3.1.1. *Let N be an odd positive integer with at least two different prime factors and let $m \in \mathbb{Z}$, $d \in \mathbb{Z}_{>0}$ and $h(X) \in \mathbb{Z}[X]$ a monic degree d polynomial satisfying the conditions 1.1. Then, if Lenstra's Hypothesis (3.2.2) is true for the polynomial h_w, there is a finite set of integers $S \subseteq \mathbb{Z}$ and an element $\beta \in B$ such that conditions 3.2 hold and* $\gcd([\Psi(\beta)], N) \notin \{1, N\}$.

3.2 The Lenstra's Hypothesis

Let $g \in \mathbb{Q}[X]$ be a monic rational polynomial with discriminant $\Delta(g) \neq 0$ and positive degree. Let also

$$F := \mathbb{Q}[X]/g\mathbb{Q}[X] = \mathbb{Q}[\omega] \text{ where } \omega := (X \bmod g) \in F.$$

If p is a prime number, we denote as usual with $\mathbb{Q}_p$ the field of p-adic numbers, with $\mathbb{Z}_p$ the ring of p-adic integers, and we have as in the previous section

$$F_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} F = \mathbb{Q}_p[\omega] = \mathbb{Q}_p[X]/g\mathbb{Q}_p[X].$$

It is easy to see that F_p contains F as subring via the natural inclusion

$$\begin{aligned} F &\hookrightarrow F_p \\ h(X) &\mapsto h(X) \end{aligned}$$

which actually restricts to a group morphism between the invertible elements $F^* \hookrightarrow F_p^*$.

Lemma 3.2.1. *Let F and ω be defined as above. Then for every rational $b \in \mathbb{Q}$ the element $(\omega - b)$ is invertible in F if and only if $g(b) \neq 0$.*

Proof. By the polynomial division with remainder in $\mathbb{Q}[X]$ we have

$$g(X) = (X - b)l(X) + g(b).$$

If b is not a zero of g, we have $(\omega - b)^{-1} = -\frac{l(\omega)}{g(b)} \in F^*$. On the other side, if b is a zero of g we get

$$0 = g(\omega) = (\omega - b)l(\omega)$$

so if $(\omega - b)$ was intertible, then $l(\omega) = 0$ contradicting $\Delta(g) \neq 0$. □

Therefore we can define J to be the subgroup of F^* given by

$$J := \left\langle \frac{\omega - a}{\omega - b} \mid a, b \in \mathbb{Z} \text{ such that } a, b > \text{any real zero of } g \right\rangle \subseteq F^*$$

and similarly let J_p be the subgroup of F_p^* defined by

$$J_p := \left\langle \frac{\omega - a}{\omega - b} \mid a, b \in \mathbb{Z}_p \text{ such that } g(a) \neq 0, g(b) \neq 0 \right\rangle \subseteq F_p^*.$$

The following hypothesis expresses the idea that the group J is in fact completely characterized by a list of local conditions in terms of the J_p's.

Hypothesis 3.2.2 (H.W. Lenstra)**.** *With the above notation, an element $\beta \in F^*$ belongs to J if and only if the following two conditions are satisfied:*

(i) $\varphi(\beta) > 0$ for every ring morphism $\varphi : F \to \mathbb{R}$.

(ii) for every prime p the image of β under $F^* \hookrightarrow F_p^*$ belongs to J_p.

3.3 Local properties

Here we want to discuss a couple of properties of the J_p's and give a more compact formulation of the Hypothesis 3.2.2. Let f be as in the first section the polynomial defining $F = \mathbb{Q}[\omega]$ and $n := \deg f$. Recall that all the valuations on a finite dimensional vector space over a complete field are equivalent (chapter 2, [CF67]), then the following $\mathbb{Q}_p$-linear map

$$\begin{aligned} (\mathbb{Q}_p)^n &\xrightarrow{\sim} F_p \\ (c_0, \dots, c_{n-1}) &\mapsto \sum_{i=0}^{n-1} c_i \omega^i + \omega^n \end{aligned}$$

is really an isomorphism of topological spaces. Consider on $(\mathbb{Q}_p)^n$ the valuation given by

$$|(c_0, \dots, c_{n-1})|_\infty = \max\{|c_i| \mid 0 \le i \le n-1\}.$$

The following proposition formalizes the idea that the roots of a polynomial are continuous functions of the coefficients.

Proposition 3.3.1. *Let C_p be an algebraic closure of $\mathbb{Q}_p$ and let $|\cdot|$ be the extended valuation that inherits from $\mathbb{Q}_p$. Consider also $\prod_{i=1}^n (\omega - a_i) = \sum_{i=0}^{n-1} c_i \omega^i + \omega^n \in F_p$ with $a_i \in C$ and $c_i \in \mathbb{Q}_p$. Then for every $\epsilon > 0$ there exists $\delta > 0$ such that for every $\prod_{j=1}^n (\omega - b_j) = \sum_{j=0}^{n-1} d_j \omega^j + \omega^n \in F_p$ we have, up to permuting the b_j's,*

$$|(c_0, \dots, c_{n-1}) - (d_0, \dots, d_{n-1})|_\infty < \delta \Rightarrow \ \forall\ 1 \le i \le n : |a_i - b_i| < \epsilon.$$

Proof. See chapter 2, [Art67]. □

The following is the first important result about the J_p's that we will need.

Proposition 3.3.2. *For every place p of $\mathbb{Q}$, the subset $J_p \subseteq F_p^* = \prod_{\mathfrak{p}|p} F_{\mathfrak{p}}^*$ is open.*

Proof. Let $a_1, \dots, a_n$ be pairwise distinct elements of $\mathbb{Z}_p$ such that $f(a_i) \neq 0$ for every $1 \le i \le n$. Consider the element $\zeta := \prod_{i=1}^n (\omega - a_i) = \sum_{i=0}^{n-1} c_i \omega^i + \omega^n \in F_p$. Let also as above C_p be an algebraic closure of $\mathbb{Q}_p$ and $Z := \{x \in C_p \mid f(x) = 0\}$ be the finite set of zeros of f in C_p. Define

$$\epsilon_1 := \min\left\{ \frac{|a_i - a_j|}{2} \mid 1 \le i, j \le n,\ i \neq j \right\}, \quad \epsilon_2 := \min\{|a_i - x| \mid 1 \le i \le n,\ x \in Z\}$$

and

$$\epsilon := \frac{\min\{1, \epsilon_1, \epsilon_2\}}{2} > 0.$$

By Proposition 3.3.1 there is $\delta > 0$ such that if we define an open neighbourhood of ζ as

$$U := \{x \in F_p \mid |x - \zeta| < \delta\}$$

then every element $\sum_{i=0}^{n-1} d_i \omega^i + \omega^n$ of U can be written as $\prod_{i=1}^n (\omega - b_i)$ with $b_i \in C_p$ pairwise distinct (by the choice of ϵ_1) and $f(b_i) \neq 0$ (by the choice of ϵ_2). Since, by the uniqueness of the extended valuation to an algebraic closure, the valuation is stable under the action of the Galois group, we have $|a_i - \sigma(b_i)| < \epsilon$ so $\sigma(b_i) = b_i$ for every σ in $\mathrm{Gal}(C_p|\mathbb{Q}_p)$, i.e. $b_i \in \mathbb{Q}_p$. Moreover, since by definition $\epsilon < 1$ and $a_i \in \mathbb{Z}_p$, also b_i lies then in $\mathbb{Z}_p$. Thus, $\zeta^{-1} \cdot U \subseteq J_p$ is a non-empty open subset, so by Lemma 2.2.4 we conclude that J_p is open. □

The second proposition we need requires some results that we do not include here. We provide nevertheless a sketch of the proofs of this proposition and of the next theorem, which is a fundamental tool for proving the required result.

Theorem 3.3.3. *Let $f \in \mathbb{F}_p[X]$ be a monic polynomial of degree $n = \deg f$. If $p > n^2$, then*

$$(\mathbb{F}_p[X]/f\mathbb{F}_p[X])^* = \left\langle \left(\frac{X-a}{X-b} \bmod f\right) \mid a, b \in \mathbb{F}_p, f(a) \neq 0, f(b) \neq 0 \right\rangle.$$

Sketch of the proof. Let as usual $\mathbb{F}_p[\alpha] := \mathbb{F}_p[X]/f\mathbb{F}_p[X]$ for $\alpha := (X \bmod f)$. Assume by contradiction that the statement is not true; then there is a non-trivial character

$$1 \neq \chi : (\mathbb{F}_p[\alpha])^* \to \mathbb{C}^*$$

that is trivial on the subgroup $\langle (\frac{X-a}{X-b} \bmod f) \mid a, b \in \mathbb{F}_p, f(a) \neq 0, f(b) \neq 0 \rangle$ of $(\mathbb{F}_p[\alpha])^*$, i.e. $\chi(\alpha - a) = \chi(\alpha - b)$ for every $a, b \in \mathbb{F}_p$ such that $f(a) \neq 0$ and $f(b) \neq 0$. It is a fact (see [Wei74]) that in this setting

$$\sum_{g \in \mathbb{F}_p[X] \text{ monic}} \chi\big((g \bmod f)\big) T^{\deg g} = \prod_{i=1}^{n-1} (1 - w_i T)$$

with w_i complex numbers such that $|w_i| \leq \sqrt{p}$. If we now look at the absolute value of the coefficient of T in the above equation we get

$$|-\sum_{i=1}^{n-1} w_i| = |\sum_{\substack{a \in \mathbb{F}_p \\ f(a) \neq 0}} \chi(\alpha - a)| = \#\{a \in \mathbb{F}_p \mid f(a) \neq 0\}$$

where the last equality follows from the choice of χ. Then we have the inequalities

$$(n-1) \cdot \sqrt{p} \geq |-\sum_{i=1}^{n-1} w_i| = \#\{a \in \mathbb{F}_p \mid f(a) \neq 0\} \geq p - n$$

that leads to a contradiction since $p > n^2$. □

Proposition 3.3.4. *The set*

$$T := \left\{ p \text{ is an integer prime} \mid J_p \neq \prod_{\substack{\mathfrak{p} \mid p \\ F_\mathfrak{p} = \mathbb{Q}_p}} F_\mathfrak{p}^* \times \prod_{\substack{\mathfrak{p} \mid p \\ F_\mathfrak{p} \neq \mathbb{Q}_p}} \mathcal{O}_{F_\mathfrak{p}}^* \right\}$$

is finite.

Sketch of the proof. Let

$$T_1 := \{p \text{ is an integer prime} \mid p \text{ divides some denominator of a coefficient of } f\}$$

and

$$T_2 := \{p \text{ is an integer prime} \mid \operatorname{ord}_p \Delta(f) > 0\}.$$

If $p \notin T_1$ then $\mathbb{Z}_p[\omega] = \bigoplus_{i=0}^{n-1} \mathbb{Z}_p \cdot \omega^i$ and if $p \notin T_1 \cup T_2$ then $\bigoplus_{i=0}^{n-1} \mathbb{Z}_p \cdot \omega^i = \prod_{\mathfrak{p}|p} \mathcal{O}_{F_\mathfrak{p}}$. Moreover, let

$$T_3 := \{p \text{ is an integer prime} \mid p \leq 2n\}.$$

When $p \notin T_1 \cup T_2 \cup T_3$ we have $1 + p\mathbb{Z}_p[\omega] \subseteq J_p$. Then, outside the finite set

$$T := T_1 \cup T_2 \cup T_3$$

we have

$$\prod_{\substack{\mathfrak{p}|p \\ F_\mathfrak{p}=\mathbb{Q}_p}} F_\mathfrak{p}^* \times \prod_{\substack{\mathfrak{p}|p \\ F_\mathfrak{p}\neq\mathbb{Q}_p}} \mathcal{O}_{F_\mathfrak{p}}^* \supseteq \prod_{\mathfrak{p}|p} \mathcal{O}_{F_\mathfrak{p}}^* = \mathbb{Z}_p[\omega]^* \supseteq 1 + p\mathbb{Z}_p[\omega] \subseteq J_p.$$

Since J_p sits in $\prod_{\substack{\mathfrak{p}|p \\ F_\mathfrak{p}=\mathbb{Q}_p}} F_\mathfrak{p}^* \times \prod_{\substack{\mathfrak{p}|p \\ F_\mathfrak{p}\neq\mathbb{Q}_p}} \mathcal{O}_{F_\mathfrak{p}}^*$, we just need to prove that it contains every representative of the quotient group

$$\Big(\prod_{\substack{\mathfrak{p}|p \\ F_\mathfrak{p}=\mathbb{Q}_p}} F_\mathfrak{p}^* \times \prod_{\substack{\mathfrak{p}|p \\ F_\mathfrak{p}\neq\mathbb{Q}_p}} \mathcal{O}_{F_\mathfrak{p}}^* \Big) / (1 + p\mathbb{Z}_p[\omega]).$$

We do this in two steps. We first observe that it fills the representatives of $1 + p\mathbb{Z}_p[\omega]$ in $\mathbb{Z}_p[\omega]^*$: since

$$(\mathbb{Z}_p[\omega]^*)/(1 + p\mathbb{Z}_p[\omega]) \simeq \mathbb{F}_p[\omega]^*$$

what we need follows from Theorem 3.3.3. Afterwards, we prove that J_p fills also all the representatives of

$$\Big(\prod_{\substack{\mathfrak{p}|p \\ F_\mathfrak{p}=\mathbb{Q}_p}} F_\mathfrak{p}^* \times \prod_{\substack{\mathfrak{p}|p \\ F_\mathfrak{p}\neq\mathbb{Q}_p}} \mathcal{O}_{F_\mathfrak{p}}^* \Big) / (\prod_{\mathfrak{p}|p} \mathcal{O}_{F_\mathfrak{p}}^*) \simeq \mathbb{Z}^{\{\mathfrak{p} \mid F_\mathfrak{p}=\mathbb{Q}_p\}} \tag{3.3}$$

where the isomorphism is given by the valuation maps. This amounts to saying that we can find inside J_p elements of any prescribed valuation. Since, for a fixed $\mathfrak{p}$, we can always find $b \in \mathbb{Z}_p$ such that

$$\mathrm{ord}_\mathfrak{p}(\omega - b) = 0$$

it is sufficient to show that $\mathrm{ord}_\mathfrak{p}(\omega - a) = 1$ for some $a \in \mathbb{Z}_p$, because then $\mathrm{ord}_\mathfrak{p}(\frac{\omega-a}{\omega-b}) = 1$. Let us consider any $a \in \mathbb{Z}_p$ such that $\mathrm{ord}_\mathfrak{p}(\omega - a) > 0$; if the order is 1 we finished, otherwise pick $a' := a + p$ and $\mathrm{ord}_\mathfrak{p}(\omega - a')$ will be 1. □

To formulate the Hypothesis 3.2.2 in a more compact form, let us define as for the p-adic case $F_\infty := \mathbb{R} \otimes_\mathbb{Q} F \simeq \mathbb{Q}_p[\omega]$, and

$$J_\infty := (F_\infty^*)^2.$$

Lemma 3.3.5. *With the notation introduced in the previous section, the Hypothesis 3.2.2 is equivalent to the following equality of sets*

$$J = \Big(F^* \cap \prod_{p \leq \infty} J_p \Big) \subseteq \Big(F^* \cap \prod_{p \leq \infty} F_p^* \Big).$$

Proof. We saw in Chapter 2 that $F_\infty = \prod_{\mathfrak{p}|\infty} F_\mathfrak{p}$ where each $F_\mathfrak{p}$ is $\mathbb{R}$ or $\mathbb{C}$, depending on the degree of the corresponding irreducible factor of f over $\mathbb{R}[X]$. The ring morphisms $F \to \mathbb{R}$ correspond exactly to the real zeros of f, i.e. to $\mathfrak{p}|\infty$ whith $F_\mathfrak{p} = \mathbb{R}$, so the condition (i) of the Hypothesis amounts to saying that in each such coordinate the element $\beta \in F^*$ is positive. Since being positive is equivalent to being a non-zero square in $\mathbb{R}$, and being a square in $\mathbb{C}$ is an empty condition, for every $\beta = (\beta_p)_{p\leq\infty} \in F^*$ we have

$$\text{condition (i) of Hypothesis 3.2.2 holds} \iff \beta_\infty \in \prod_{\mathfrak{p}|\infty} (F_\mathfrak{p}^*)^2 = J_\infty \tag{3.4}$$

and, in view of Proposition 3.3.4, we also have

$$\text{condition (ii) Hypothesis 3.2.2 holds} \iff (\beta_p)_{p<\infty} \in \prod_{p<\infty} J_p. \tag{3.5}$$

The equivalences 3.4 and 3.5 together give the result. □

3.4 Non-triviality of the gcd

In this section we will give a sufficient condition on the β of the Theorem 3.1.1 such that it satisfies $\gcd([\Psi(\beta)], N) \notin \{1, N\}$.

Let $Q := \{p \text{ positive integer prime} \mid p|N\}$ and $e_p := \mathrm{ord}_p(N)$, so the positive prime factorization of N is given by

$$N = \prod_{p\in Q} p^{e_p}.$$

In the following we will need to distinguish one element of Q from the others. For the sake of minimality, we just choose the minimal one, i.e.

$$q := \min\{p \mid p \in Q\}.$$

The Chinese Remainder Theorem gives us $\mathbb{Z}/N\mathbb{Z} \simeq \prod_{p\in Q} \mathbb{Z}/p^{e_p}\mathbb{Z}$, which clearly restricts to the unit groups of both rings. We will then identify

$$\begin{aligned}(\mathbb{Z}/N\mathbb{Z})^* \times (\mathbb{Z}/N\mathbb{Z})^* &\xrightarrow{\sim} \prod_{p\in Q} (\mathbb{Z}/p^{e_p}\mathbb{Z})^* \times (\mathbb{Z}/p^{e_p}\mathbb{Z})^* \\ (a, b) &\mapsto (a_p, b_p)_{p\in Q}.\end{aligned}$$

Let us consider a particular element of $(\mathbb{Z}/N\mathbb{Z})^* \times (\mathbb{Z}/N\mathbb{Z})^*$, namely

$$\delta := (1, \epsilon_p)_{p\in Q} \text{ where } \epsilon_p = \begin{cases} -1 & \text{if } p = q \\ 1 & \text{if } p \neq q. \end{cases} \tag{3.6}$$

We now go back to the Ψ defined in the first section: it can be realized as a composition of two group morphisms, namely

$$\begin{array}{ccccc} B \simeq \mathbb{Z} \times C & \xrightarrow{\psi=(\psi_1,\psi_2)} & \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} & \xrightarrow{\varphi=\left((a,b)\mapsto a-b\right)} & \mathbb{Z}/N\mathbb{Z} \\ (n, c) & \longmapsto & \big(\psi_1(n), \psi_2(c)\big) & \longmapsto & \psi_1(n) - \psi_2(c). \end{array}$$

Recall that the N of our interest has at least two different positive prime factors different from 2. We now prove that under this assumptions any element $\beta \in B$ that is mapped to δ under ψ gives rise to a non-trivial factor of N.

Lemma 3.4.1. *Let $\beta \in B$ such that $\psi(\beta) = \delta \in (\mathbb{Z}/N\mathbb{Z})^* \times (\mathbb{Z}/N\mathbb{Z})^*$. If $N \in \mathbb{Z}_{>0}$ is odd with at least two different positive prime factors, then* $\gcd([\Psi(\beta)], N)$ *is a non-trivial factor of N.*

Proof. Since $\#Q \geq 2$ we can pick an $r \in Q \setminus \{q\}$ (e.g. $r := \max\{p \mid p \in Q\}$). Therefore we have

$$\Psi(\beta) = (\varphi \circ \psi)(\beta) = \varphi(\delta) = (k_p)_{p \in Q} \in \mathbb{Z}/N\mathbb{Z}$$

where

$$\begin{aligned} k_q &\equiv 1 - (-1) \equiv 2 \bmod q^{e_q} \\ k_r &\equiv 1 - 1 \equiv 0 \bmod r^{e_r} \end{aligned}$$

so $[\Psi(\beta)]$ is an integer that is divisible by r but not by q, since 2 is a unit in $\mathbb{Z}/q^{e_q}\mathbb{Z}$ (because N is odd, so $q \neq 2$). Then $r | \gcd([\Psi(\beta)], N)$ but $rq \nmid \gcd([\Psi(\beta)], N)$, proving the statement. □

3.5 Proof of the result

In this section we prove Theorem 3.1.1; the proof consists of making use of the Lenstra's Hypothesis (3.2.2) to express the problem in terms of finding an element $\zeta \in F^*$ with some prescribed properties, which existence will follow by applying the Degree One Theorem (2.1.2).

Consider again the factorization $\Psi = \varphi \circ \psi$ as in the previous section. Since the map ψ is surjective (because both ψ_1 and ψ_2 are), we can always find elements $\beta \in B$ satisfying the hypotheses of Lemma 3.4.1. It still remains to be proved that we can find such an element that also satisfies the conditions 3.2.

Let us now focus on the ψ morphism: it is actually a ring homomorphism, and its kernel is given by the ideal $\mathfrak{n}_0 \times \mathfrak{n}_1 := N\mathbb{Z} \times (N, \gamma - m)C$. We can factor this map through the completion $\widehat{B}_{\mathfrak{n}_0 \times \mathfrak{n}_1}$ of B with respect to $\mathfrak{n}_0 \times \mathfrak{n}_1$, obtaining a map $\psi' : \widehat{B}_{\mathfrak{n}_0 \times \mathfrak{n}_1} \to \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ such that the following diagram

$$\begin{tikzcd} B \arrow[rr, two heads, "\psi=(\psi_1,\psi_2)"] \arrow[dr] & & \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \\ & \widehat{B}_{\mathfrak{n}_0 \times \mathfrak{n}_1} \arrow[ur, two heads, "\psi'"'] & \end{tikzcd} \tag{3.7}$$

commutes. For some reasons that will be clarified later, we would like to restrict our maps to reach only the invertible elements in $\mathbb{Z}/N\mathbb{Z}$. This is possible, according to the following lemma.

Lemma 3.5.1. *Let A, B be commutative rings and $f : A \to B$ a surjective ring homomorphism with kernel $I := \ker f$. Then every element of A that is mapped to B^* by f is invertible in the completion $\widehat{A}_I$.*

Proof. Let $a \in A$ be an element whose image $f(a)$ is invertible, i.e. (being f surjective) there is an element $a' \in A$ such that $f(a)f(a') = 1 \in B$, which implies

$$x := 1 - aa' \in I.$$

Then we have

$$\begin{aligned}(a)_{n\in\mathbb{N}} \cdot \big(a' \sum_{j=0}^{n} x^j\big)_{n\in\mathbb{N}} &= aa'\big(\sum_{j=0}^{n} x^j\big)_{n\in\mathbb{N}} \\ &= (1-x)\big(\sum_{j=0}^{n} x^j\big)_{n\in\mathbb{N}} = (1-x^{n+1})_{n\in\mathbb{N}} = (1)_{n\in\mathbb{N}} \in \widehat{A}_I\end{aligned}$$

so the element $\big(a' \sum_{j=0}^{n} x^j\big)_{n\in\mathbb{N}} \in \widehat{A}_I$ is the inverse of $(a)_{n\in\mathbb{N}} \in \widehat{A}_I$. □

We will call

$$B_{\text{cop}} := \{b \in B \mid \psi(b) \in (\mathbb{Z}/N\mathbb{Z})^* \times (\mathbb{Z}/N\mathbb{Z})^*\} \subseteq B$$

the elements of B that are mapped to units by ψ. By Lemma 3.5.1 the restricted map $\iota : B_{\text{cop}} \to \widehat{B}^*_{\mathfrak{n}_0\times\mathfrak{n}_1}$ is well-defined, then we can restrict the whole diagram 3.7 to

$$\begin{tikzcd} B_{\text{cop}} \arrow[rr, two heads, "\psi=(\psi_1,\psi_2)"] \arrow[dr, "\iota"'] & & (\mathbb{Z}/N\mathbb{Z})^* \times (\mathbb{Z}/N\mathbb{Z})^* \\ & \widehat{B}^*_{\mathfrak{n}_0\times\mathfrak{n}_1} \arrow[ur, two heads, "\psi'"'] & \end{tikzcd}$$

where we denote for convenience the restricted maps with the same names as the original ones. Define now the set

$$\Gamma := \{\mathfrak{p} \in \text{Maxspec}B \mid \mathfrak{p} \supseteq \mathfrak{n}_0 \times \mathfrak{n}_1\}.$$

This Γ is finite, because it is well-known that there is an inclusion preserving correspondence between the ideals of Γ and the maximal ideals of $B/\mathfrak{n}_0\times\mathfrak{n}_1 \simeq \mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}$, which are finite in number. Moreover, since every maximal ideal of $\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}$ is of the form $p\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ or $\mathbb{Z}/N\mathbb{Z} \times p\mathbb{Z}/N\mathbb{Z}$ for some $p \mid N$, we will say that the corresponding ideal $\mathfrak{p} \in \Gamma$ is above p, and we will denote it with $\mathfrak{p}|p$.

Lemma 3.5.2. *With the definition introduced above, we have a natural ring isomorphism*

$$\widehat{B}_{\mathfrak{n}_0\times\mathfrak{n}_1} \simeq \prod_{\mathfrak{p}\in\Gamma} \widehat{B}_{\mathfrak{p}}.$$

Proof. Since $\mathfrak{p} \in \Gamma$ are maximal ideals, the Chinese Remainder Theorem gives us

$$\prod_{\mathfrak{p}\in\Gamma} \widehat{B}_{\mathfrak{p}} \simeq \widehat{B}_{(\prod_{\mathfrak{p}\in\Gamma}\mathfrak{p})}.$$

To prove that the two completions of B, with respect to the ideals $\mathfrak{n}_0 \times \mathfrak{n}_1$ and $\prod_{\mathfrak{p}\in\Gamma}\mathfrak{p}$, are naturally isomorphic it is sufficient to prove that the powers of $\mathfrak{n}_0 \times \mathfrak{n}_1$ and the powers of $\prod_{\mathfrak{p}\in\Gamma}\mathfrak{p}$ are two cofinal filtrations, i.e. that for every $i \in \mathbb{Z}_{>0}$ there exists $j \in \mathbb{Z}_{>0}$

such that $(\prod_{\mathfrak{p}\in\Gamma}\mathfrak{p})^j \subseteq (\mathfrak{n}_0\times\mathfrak{n}_1)^i$ and for every $j\in\mathbb{Z}_{>0}$ there exists $i\in\mathbb{Z}_{>0}$ such that $(\mathfrak{n}_0\times\mathfrak{n}_1)^i \subseteq (\prod_{\mathfrak{p}\in\Gamma}\mathfrak{p})^j$ (see chapter 7, [Eis95]).

The ideal $\mathfrak{n}_0\times\mathfrak{n}_1$ corresponds to the zero ideal in $\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}$ and $\prod_{\mathfrak{p}\in\Gamma}\mathfrak{p}$ corresponds to the ideal $\mathrm{rad}(N)\cdot(\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z})$, where $\mathrm{rad}(N):=\prod_{p|N}p$. Since the correspondence is inclusion preserving, we clearly have

$$\mathfrak{n}_0\times\mathfrak{n}_1 \subseteq \prod_{\mathfrak{p}\in\Gamma}\mathfrak{p}$$

and if we let $M=\max_{p|N}\{\mathrm{ord}_p(N)\}$, we also get $\left(\prod_{\mathfrak{p}\in\Gamma}\mathfrak{p}\right)^M=(0)\subseteq B/\mathfrak{n}_0\times\mathfrak{n}_1$, which means

$$\Big(\prod_{\mathfrak{p}\in\Gamma}\mathfrak{p}\Big)^M \subseteq \mathfrak{n}_0\times\mathfrak{n}_1.$$

From the above inclusions the cofinality follows, giving us the required isomorphism of rings. □

We will see from now on the above isomorphism as an identification.

Lemma 3.5.3. *For every $\mathfrak{p}\in\Gamma$, the ring $\widehat{B}_{\mathfrak{p}}$ is isomorphic to the ring of integers of the corresponding $F_{\mathfrak{p}}$.*

Proof. By Lemma 3.5.2 and since B is a finitely generated $\mathbb{Z}$-module we have

$$\prod_{\mathfrak{p}|p}\widehat{B}_{\mathfrak{p}} \simeq \widehat{B}_{p\mathbb{Z}} \simeq B\otimes_{\mathbb{Z}}\widehat{\mathbb{Z}}_{p\mathbb{Z}} = B\otimes_{\mathbb{Z}}\mathbb{Z}_p.$$

We also know that for a number field F with ring of integers B we have the natural isomorphism

$$F\simeq B\otimes_{\mathbb{Z}}\mathbb{Q}.$$

Since the tensor product commutes with finite sums, it also holds for finite étale algebras over $\mathbb{Q}$. Therefore we have

$$\prod_{\mathfrak{p}|p}F_{\mathfrak{p}} = F\otimes_{\mathbb{Q}}\mathbb{Q}_p \simeq (B\otimes_{\mathbb{Z}}\mathbb{Q})\otimes_{\mathbb{Q}}\mathbb{Q}_p \simeq (B\otimes_{\mathbb{Z}}\mathbb{Z}_p)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p \simeq \prod_{\mathfrak{p}|p}\big(\widehat{B}_{\mathfrak{p}}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p\big).$$

Hence each $F_{\mathfrak{p}}$ corresponds to some $\widehat{B}_{\mathfrak{p}}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p\simeq\mathrm{Frac}\,\widehat{B}_{\mathfrak{p}}$. □

Under the ring isomorphisms (which restrict to group isomorphisms of the unit groups) given by Lemma 3.5.2 and Lemma 3.5.3, we can the embed $\widehat{B}^*_{\mathfrak{n}_0\times\mathfrak{n}_1}$ inside $\prod_{\mathfrak{p}\in\Gamma}F^*_{\mathfrak{p}}$.

Set $\omega:=\frac{\alpha-m-1}{N}$ and let h_ω be the minimal polynomial of ω over $\mathbb{Q}$, which exists since α was integral (hence algebraic) over $\mathbb{Q}$, and let J be defined as in Section 3.2, i.e.

$$\begin{aligned} J &= \left\langle \frac{a-\omega}{b-\omega} \mid a,b\in\mathbb{Z} \text{ such that } a,b>\text{any real zero of } h_\omega \right\rangle \\ &= \left\langle \frac{m+1+Na-\alpha}{m+1+Nb-\alpha} \mid a,b\in\mathbb{Z} \text{ such that } a,b>\text{any real zero of } h_\omega \right\rangle. \end{aligned}$$

The following proposition reduces the proof of the Theorem 3.1.1 to check an algebraic condition.

Proposition 3.5.4. *Suppose that Hypothesis 3.2.2 is true for the polynomial h_w. With the notation as in the previous sections, if there exists an element $\zeta \in F^*$ such that*

(i) When we see ζ inside $\prod_{\mathfrak{p}\in\Gamma} F^*_{\mathfrak{p}}$, it belongs to $\widehat{B}^*_{\mathfrak{n}_0\times\mathfrak{n}_1}$ and has image δ under ψ'

(ii) $\zeta^2 \in F^* \cap \prod_{p\leq\infty} J_p$

then Theorem 3.1.1 holds.

Proof. Clearly $\mathbb{Q}[\alpha] = \mathbb{Q}[\omega]$, so we may apply the Lenstra's Hypothesis on the polynomial h_w as in the Lemma 3.3.5 obtaining

$$F^* \cap \prod_{p\leq\infty} J_p = J.$$

Then the condition $\zeta^2 \in F^* \cap \prod_{p\leq\infty} J_p$ is equivalent to

$$\zeta^2 = \frac{m+1+Na_1-\alpha}{m+1+Nb_1-\alpha}\cdots\frac{m+1+Na_t-\alpha}{m+1+Nb_t-\alpha}$$

for some $t \in \mathbb{Z}_{>0}$ and integers $\{a_j, b_j\}_{j=1,\ldots,t}$ greater then any real zero of h_ω. If we define the element

$$\beta := \zeta\prod_{j=1}^{t}(m+1+Nb_j-\alpha) \in F^*$$

it satisfies

$$\beta^2 = \prod_{j=1}^{t}(m+1+Na_j-\alpha)(m+1+Nb_j-\alpha) \in \mathbb{Z}[\alpha].$$

Then β is integral over $\mathbb{Z}[\alpha]$ so it is integral over $\mathbb{Z}$, i.e. $\beta \in B$. If we apply the ring morphism ψ to this β we get

$$\begin{aligned}\psi(\beta) &= (\psi'\circ\iota)\Big(\zeta\cdot\prod_{j=1}^{t}(m+1+Nb_j-\alpha)\Big) = \psi'\Big(\zeta\cdot\iota\Big(\prod_{j=1}^{t}(m+1+Nb_j-\alpha)\Big)\Big)\\ &= \psi'(\zeta)\cdot\psi\Big(\prod_{j=1}^{t}(m+1+Nb_j-\alpha)\Big) = \psi'(\zeta)\cdot(1,1) = \delta\end{aligned}$$

because by definition of ψ we have

$$\psi(\alpha) = \big(\psi_1(m), \psi_2(\gamma)\big) = (m, m).$$

Then by Lemma 3.4.1 we know that $\gcd([\Psi(\beta)], N)$ is a non-trivial factor of N. We also clearly see that β satisfies the conditions 3.2 together with the set

$$S := \{m+1+Na_j\}_{j=1,\ldots,t} \cup \{m+1+Nb_j\}_{j=1,\ldots,t}$$

and this proves Theorem 3.1.1. □

As we saw in Chapter 2, on $\widehat{B}_{\mathfrak{p}}$ we have the $\widehat{\mathfrak{p}}$-adic topology, where $\widehat{\mathfrak{p}}$ is the ideal generated by $\mathfrak{p}$ in $\widehat{B}_{\mathfrak{p}}$ or, equivalentely, $\widehat{\mathfrak{p}} = \widehat{B}_{\mathfrak{p}} \otimes_B \mathfrak{p}$. Moreover, $\widehat{B}_{\mathfrak{p}}^*$ is a topological group, and the subgroup

$$V := \prod_{\substack{\mathfrak{p}\in\Gamma \\ \mathfrak{p}|p}} (1 + \hat{\mathfrak{p}}^{e_p}) \subseteq \prod_{\mathfrak{p}\in\Gamma} \widehat{B}_{\mathfrak{p}}^*$$

is open in the product topology. This V is in fact the kernel of the surjective morphism ψ', so

$$\big(\prod_{\mathfrak{p}\in\Gamma} \widehat{B}_{\mathfrak{p}}^*\big)/V \simeq (\mathbb{Z}/N\mathbb{Z})^* \times (\mathbb{Z}/N\mathbb{Z})^*. \tag{3.8}$$

We are finally ready to prove the main theorem of this work.

Proof of Theorem 3.1.1. In the view of Proposition 3.5.4 it suffices to show that we can always construct a $\zeta \in F^*$ satisfying (i) and (ii) of that proposition. Consider the coset δV in $\prod_{\mathfrak{p}\in\Gamma} \widehat{B}_{\mathfrak{p}}^*$ corresponding under the isomorphism 3.8 to the δ defined in 3.6. Let also

$$S := \{p \in \mathbb{Z}_{>0} \mid p \text{ is a prime dividing } N\} \cup \{\infty\} \cup T$$

where $T := \left\{ p \text{ is an integer prime} \mid J_p \neq \prod_{\substack{\mathfrak{p}|p \\ F_{\mathfrak{p}}=\mathbb{Q}_p}} F_{\mathfrak{p}}^* \times \prod_{\substack{\mathfrak{p}|p \\ F_{\mathfrak{p}}\neq\mathbb{Q}_p}} \mathcal{O}_{F_{\mathfrak{p}}}^* \right\}$ as in Proposition 3.3.4; by that proposition, the set S is finite (and contains ∞). By Proposition 3.3.2 we also know that the J_p are open in $F_p^* = \prod_{\mathfrak{p}|p} F_{\mathfrak{p}}^*$, so for every $p \in S$ the Lemma 2.2.5 tells us that J_p contains a product of open subgroups $H_{\mathfrak{p}} \subseteq F_{\mathfrak{p}}^*$. Define then

$$I_{\mathfrak{p}} := \begin{cases} H_{\mathfrak{p}} & \text{if } \mathfrak{p} \notin \Gamma \\ \delta_{\mathfrak{p}} \cdot \big(H_{\mathfrak{p}} \cap (1 + \hat{\mathfrak{p}}^{e_p})\big) & \text{if } \mathfrak{p} \in \Gamma. \end{cases}$$

Finally, we define

$$U := \prod_{p\in S} \big(\prod_{\mathfrak{p}|p} I_{\mathfrak{p}}\big) \subseteq \prod_{p\in S} \big(\prod_{\mathfrak{p}|p} F_{\mathfrak{p}}^*\big) = \prod_{p\in S} F_p^*.$$

The set U defined above is the coset of the open subgroup

$$\prod_{p\in S} \Big(\prod_{\substack{\mathfrak{p}\in\Gamma \\ \mathfrak{p}|p}} (H_{\mathfrak{p}} \cap V) \times \prod_{\substack{\mathfrak{p}\notin\Gamma \\ \mathfrak{p}|p}} H_{\mathfrak{p}} \Big) \subseteq \prod_{p\in S} F_p^*$$

represented by the element

$$(\underline{\delta}_{\mathfrak{p}})_{\left\{\substack{\mathfrak{p}|p \\ p\in S}\right\}} \text{ where } \underline{\delta}_{\mathfrak{p}} := \begin{cases} 1 & \text{if } \mathfrak{p} \notin \Gamma \\ \delta_{\mathfrak{p}} & \text{if } \mathfrak{p} \in \Gamma. \end{cases}$$

We can then apply the main theorem of the previous chapter (i.e. Theorem 2.1.2) to S and U just defined and get the existence of

$$\zeta = (\zeta_{\mathfrak{p}})_{\left\{\substack{\mathfrak{p}|p \\ p\leq\infty}\right\}} \in F^* \cap \Big(U \times \prod_{p\notin S} \Big(\prod_{\substack{\mathfrak{p}|p \\ F_{\mathfrak{p}}=\mathbb{Q}_p}} F_{\mathfrak{p}}^* \times \prod_{\substack{\mathfrak{p}|p \\ F_{\mathfrak{p}}\neq\mathbb{Q}_p}} \mathcal{O}_{F_{\mathfrak{p}}}^* \Big) \Big)$$

and since $S \supseteq T$ by its definition, we have

$$\zeta \in F^* \cap \Big(U \times \prod_{p \notin S} J_p\Big).$$

By the choice of U we have for every $\mathfrak{p}|p$ with $p \in S$ (so in particular for every $\mathfrak{p} \in \Gamma$, because S contains the prime divisors of N) that

$$\zeta_{\mathfrak{p}} \in \delta_{\mathfrak{p}} \cdot (H_{\mathfrak{p}} \cap V) \subseteq \delta_{\mathfrak{p}} V.$$

Hence ζ belongs to the coset δV when it is seen inside $\prod_{\mathfrak{p} \in \Gamma} F_{\mathfrak{p}}^*$, then

$$\psi'(\zeta) = \delta.$$

Finally, since $\delta^2 = (1,1)_{p \in Q} \in (\mathbb{Z}/N\mathbb{Z})^* \times (\mathbb{Z}/N\mathbb{Z})^*$, we have by the very definition of U that

$$\forall\ \mathfrak{p} : (\zeta_{\mathfrak{p}})^2 \in H_{\mathfrak{p}}$$

so, since $\prod_{\mathfrak{p}|p} H_{\mathfrak{p}} \subseteq J_p$ by definition of the $H_{\mathfrak{p}}$'s, we have

$$(\zeta)^2 \in \prod_{p \leq \infty} J_p$$

and this concludes the proof. $\square$

Appendix A

Some examples of the Lenstra's Hypothesis

In this appendix we discuss some easy cases of the Lenstra's Hypothesis stated in Section 3.2. Although nothing about its validity will be proved here, we hope that the reader can get from them at least the feeling that the statement does not sound so unreasonable.

A.1 First example

Let $f(X) = X^2 - X = X \cdot (X-1) \in \mathbb{Q}[X]$, so $\Delta(f) = 1 \neq 0$, and define $F := \mathbb{Q}[X]/f\mathbb{Q}[X] = \mathbb{Q}[\omega]$ where $\omega := (X \bmod f)$. We have the natural ring isomorphism

$$\begin{aligned} F &\xrightarrow{\sim} \mathbb{Q} \times \mathbb{Q} \\ \mathbb{Q} \ni q &\mapsto (q, q) \\ \omega &\mapsto (0, 1) \end{aligned}$$

with inverse $\big((a,b) \mapsto a + (b-a)\omega\big) : \mathbb{Q} \times \mathbb{Q} \to F$. As usual we see this isomorphism as an identification. In this setting, the J of our interest is

$$\begin{aligned} J :&= \left\langle \frac{\omega - a}{\omega - b} \mid a, b \in \mathbb{Z} \text{ such that } a, b > \text{any real zero of } f \right\rangle \\ &= \left\langle \frac{(a, a-1)}{(b, b-1)} \mid a, b \in \mathbb{Z} \text{ such that } a, b > 1 \right\rangle \subseteq F^* \end{aligned}$$

and similarly for every prime $p \in \mathbb{Z}$ we define $F_p := \mathbb{Q}_p[X]/f\mathbb{Q}_p[X] = \mathbb{Q}_p[\omega]$ and

$$\begin{aligned} J_p :&= \left\langle \frac{\omega - a}{\omega - b} \mid a, b \in \mathbb{Z}_p \text{ such that } f(a) \neq 0, f(b) \neq 0 \right\rangle \\ &= \left\langle \frac{(a, a-1)}{(b, b-1)} \mid a, b \in \mathbb{Z}_p \text{ such that } a, b \notin \{0, 1\} \right\rangle \subseteq F_p^*. \end{aligned}$$

Observe that there are only two ring morphisms $\varphi : F \to \mathbb{R}$, namely

$$\begin{aligned} \varphi_1 \text{ (resp. } \varphi_2) : F = \mathbb{Q}[\omega] &\to \mathbb{R} \\ \omega &\mapsto 0 \text{ (resp. } 1) \end{aligned}$$

which correspond, under the above identifications, to the projection morphisms

$$\begin{aligned}\varphi_1 \text{ (resp. } \varphi_2) : \mathbb{Q} \times \mathbb{Q} &\to \mathbb{R} \\ (a, b) &\mapsto a \text{ (resp. } b)\end{aligned}$$

so condition (i) of the Hypothesis is equivalent to say that an element $\beta = (a, b) \in \mathbb{Q}^* \times \mathbb{Q}^* \simeq F^*$ has positive entries.

One implication is therefore easy: for every generator $x = \frac{(a,a-1)}{(b,b-1)}$ of J we have $\varphi_1(x) = \frac{a}{b}$ and $\varphi_2(x) = \frac{a-1}{b-1}$, both positive quantities for $a, b > 1$. Moreover, the image of every such a generator of J clearly sits in J_p under the natural inclusion $F^* \hookrightarrow F_p^*$. Hence every element of J satisfies (i) and (ii) in the Hypothesis.

We are now interested in the other implication: we prove that condition (i) is sufficient to guarantee an element $(a, b) \in \mathbb{Q}^* \times \mathbb{Q}^*$ to lie in J. From what we observed above, the following lemma is exactly what we need for this purpose.

Lemma A.1.1. *As subgroups of $\mathbb{Q}^* \times \mathbb{Q}^*$, we have*

$$J = \left\langle \frac{(a, a-1)}{(b, b-1)} \mid a, b \in \mathbb{Z} \text{ such that } a, b > 1 \right\rangle = \mathbb{Q}_{>0} \times \mathbb{Q}_{>0}.$$

Proof. The inclusion $\subseteq$ is trivial. To prove the other inclusion, observe that it is sufficient to prove that for every positive prime p we have

$$(1, p),\ (p, 1) \in J.$$

We prove this claim by induction on p.

For $p = 2$ we have

$$\begin{aligned}(2,1) &= \left(\frac{(2,1)}{(3,2)}\right)^4 \cdot \left(\frac{(2,1)}{(4,3)}\right)^2 \cdot \frac{(2,1)}{(5,4)} \cdot \left(\frac{(9,8)}{(2,1)}\right)^2 \cdot \frac{(10,9)}{(2,1)} \in J \\ (1,2) &= \left(\frac{(2,1)}{(3,2)}\right)^2 \cdot \frac{(9,8)}{(2,1)} \cdot (2,1)^{-1} \in J.\end{aligned}$$

Assume now by the inductive hypothesis that for every prime p smaller than a prime $q > 2$ we have $(1, p), (p, 1) \in J$. Since both $q + 1$ and $q - 1$ are then products of primes smaller than q, we have $(\frac{q+1}{2}, 1), (1, q + 1)) \in J$, so

$$\begin{aligned}(q,1) &= \frac{(q^2, q^2-1)}{(q, q-1)} \cdot (1, q+1)^{-1} \in J \\ (1,q) &= \frac{(q+1, q)}{(2,1)} \cdot \left(\frac{q+1}{2}, 1\right)^{-1} \in J\end{aligned}$$

proving the induction step. □

As one can guess from the above solution, the key part of the problem was to write an element of the form $(n, n - 1)$ as a product of elements of J. One way to discover how do it is the following: let us consider (all) the possible pairs with entries made of primes $2, 3$ and 5, and look at their prime factorizations, as in the following table.

(x,y)	$\mathrm{ord}_2(x)$	$\mathrm{ord}_3(x)$	$\mathrm{ord}_5(x)$	$\mathrm{ord}_2(y)$	$\mathrm{ord}_3(y)$	$\mathrm{ord}_5(y)$
(2,1)	1	0	0	0	0	0
(3,2)	0	1	0	1	0	0
(4,3)	2	0	0	0	1	0
(5,4)	0	0	1	2	0	0
(6,5)	1	1	0	0	0	1
(9,8)	0	2	0	3	0	0
(10,9)	1	0	1	0	2	0
(16,15)	4	0	0	0	1	1
(25,24)	0	0	2	3	1	0
(81,80)	0	4	0	4	0	1

Now we multiply all the terms by the inverse of a given one, say $(2,1)$, obtaining

(x,y)	$\mathrm{ord}_2(x)$	$\mathrm{ord}_3(x)$	$\mathrm{ord}_5(x)$	$\mathrm{ord}_2(y)$	$\mathrm{ord}_3(y)$	$\mathrm{ord}_5(y)$
$(3,2)\cdot(2,1)^{-1}$	-1	1	0	1	0	0
$(4,3)\cdot(2,1)^{-1}$	1	0	0	0	1	0
$(5,4)\cdot(2,1)^{-1}$	-1	0	1	2	0	0
$(6,5)\cdot(2,1)^{-1}$	0	1	0	0	0	1
$(9,8)\cdot(2,1)^{-1}$	-1	2	0	3	0	0
$(10,9)\cdot(2,1)^{-1}$	0	0	1	0	2	0
$(16,15)\cdot(2,1)^{-1}$	3	0	0	0	1	1
$(25,24)\cdot(2,1)^{-1}$	-1	0	2	3	1	0
$(81,80)\cdot(2,1)^{-1}$	-1	4	0	4	0	1

The aim is to construct from these new elements any other element with entries made of primes $2,3$ and 5, for example $(2,1)$ itself. To do this, it is sufficient to find among all the nine lines in the second table six lines that generate (by adding or subtracting them componentwise) all the basis lines, i.e. the lines that have all entries equal to 0 but one equal to 1. In our case one sees that the first six lines do the work.

The same work done for primes $2,3$ and 5 can be done for every other finite set of primes. Adding a new prime in the above reasoning increases by two the number of the columns but in general by much more the number of the lines. Without any effort, one proves that it increases by at least three indeed.

Lemma A.1.2. *For a given natural number $n \geq 2$ let P_n be the set of the first n positive primes and C_n be the number of the couples $(x, x-1)$ for some $x \in \mathbb{Z}_{>1}$ such that both x and $x-1$ have only prime factors that belong to P_n. Then $C_{n+1} \geq C_n + 3$.*

Proof. Let p_{n+1} be the $(n+1)$-th positive prime. Both $(p_{n+1}+1, p_{n+1})$ and $(p_{n+1}, p_{n+1}-1)$ must have entries divisible by primes in P_{n+1} (but not all in P_n). Moreover, at least one between $(2p_{n+1}+1, 2p_{n+1})$ and $(2p_{n+1}, 2p_{n+1}-1)$ has entries divisible by primes in P_{n+1} (but not all in P_n), because if both $2p_{n+1} \pm 1$ were primes, then $2p_{n+1}$ would be divisible by 6 (since prime integers greater than 3 are ± 1 modulo 6), contradicting the fact that $p_{n+1} \geq 5$. Hence $C_{n+1} \geq C_n + 3$. □

One can try to generalize the above setting starting from an f that is product of k linear factors in $\mathbb{Q}[X]$, dealing with k-tuples instead of pairs. If tables like the above ones can still be constructed and they have (many) more lines than columns, the Hypothesis will be "probably" true also in these cases.

A.2 Second example

Let $f(X) = X^2 + 1 \in \mathbb{Q}[X]$, so $\Delta(f) = -4 \neq 0$, and define as usual $F := \mathbb{Q}[X]/f\mathbb{Q}[X] = \mathbb{Q}[\omega]$ where $\omega := (X \bmod f)$. Clearly we have $F = \mathbb{Q}(i)$ with ring of integers $\mathcal{O}_F = \mathbb{Z}[i]$; we define

$$\begin{aligned} S :&= \{p \text{ is an integer prime} \mid p \equiv 1 \bmod 4\} \\ &= \{p \text{ is an integer odd prime} \mid p = a^2 + b^2 \text{ for some } (a,b) \in \mathbb{Z}^2_{>0}\} \\ I :&= \{p \text{ is an integer prime} \mid p \equiv -1 \bmod 4\}. \end{aligned}$$

It is well-known that the prime (maximal) ideals of $\mathbb{Z}[i]$ are of three different kinds: there is $(1-i)$, which is the only prime that ramifies (over $2\mathbb{Z}$), there are $(a \pm bi)$ with $a^2+b^2 = p \in S$ which are the primes over a splitting prime $p\mathbb{Z}$ and there are (p) with $p \in I$ that are the primes over the inert primes of $\mathbb{Z}$. The unique prime factorization of $\mathbb{Z}[i]$ gives us the following equality of groups

$$F^* = \langle i \rangle \times \langle 1-i \rangle \times \langle a \pm bi \mid a^2 + b^2 = p \in S \rangle \times \langle p \mid p \in I \rangle.$$

Note that there are no ring morphisms from F to $\mathbb{R}$ i.e. the condition (i) of the Hypothesis is empty, so we just need to prove that every element of F^* belongs to J if and only if it satisfies the condition (ii). We start giving a slightly easier characterization of J.

Lemma A.2.1. *In the above setting, we have*

$$J = \langle a - i \mid a \in \mathbb{Z} \rangle.$$

Proof. We know that f has no zeros in $\mathbb{Q}$, so the definitions of J is just

$$J = \left\langle \frac{a-i}{b-i} \mid a, b \in \mathbb{Z} \right\rangle,$$

which is clearly contained in the group of the statement. But it also contains it, since for every $a \in \mathbb{Z}$ we have

$$(a - i) = \frac{(-a^2 + a - 1) - i}{(1-a) - i}$$

so the equality holds. □

We prove that both J and the set of elements of F^* satisfying condition (ii) of the Hypothesis are equal to $\langle i \rangle \times \langle 1-i \rangle \times \langle a \pm bi \mid a^2 + b^2 = p \in S \rangle$, so they are equal.

Lemma A.2.2. *Let S be the set of splitting primes of $\mathbb{Z}$ as above. Then*

$$\langle a - i \mid a \in \mathbb{Z} \rangle = \langle i \rangle \times \langle 1-i \rangle \times \langle a \pm bi \mid a^2 + b^2 = p \in S \rangle.$$

Proof. $\subseteq$) We know that $\mathbb{Z}[i] = \mathbb{Z} \oplus i \cdot \mathbb{Z}$ so an element of $\mathbb{Z}[i]$ is divisible by p if and only if both its coefficients are. Thus, the element $(a - i)$ is not divisible by any $p \in I$.
$\supseteq$) Clearly $i = \frac{1-i}{-1-i}$ and $1 - i$ belong to the LHS. Assume by contradiction that there are generators $a \pm bi$ of the RHS with $\mathbb{N}_{\mathbb{Q}(i)|\mathbb{Q}}(a \pm bi) = a^2 + b^2 = p$ that do not belong to the LHS; take one of these generators with minimal norm p. Since $(p) = (a + bi) \cdot (a - bi)$ in $\mathbb{Z}[i]$ and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ we know that the inertia degree $f\big((a \pm bi)|(p)\big)$ is 1, so we have a field isomorphism

$$\varphi : \mathbb{Z}[i]/(a \pm bi)\mathbb{Z}[i] \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}.$$

Let $(c \bmod p) := \varphi(i)$ where c is an integer that may be chosen to have absolute value $|c| \leq \frac{p}{2}$. Since $c - i \in \ker \varphi$ we get

$$(c - i) = \rho \cdot (a \pm bi) \tag{A.1}$$

for some $\rho \in \mathbb{Z}[i]$ not divisible by primes in I, so $\rho \in \langle i \rangle \times \langle 1-i \rangle \times \langle a \pm bi \mid a^2 + b^2 = p \in S \rangle$. Taking the norms in the last equation, we get

$$\left(\frac{p}{2}\right)^2 + 1 \geq c^2 + 1 = \mathbb{N}_{\mathbb{Q}(i)|\mathbb{Q}}(\rho) \cdot p$$

which implies that $\mathbb{N}_{\mathbb{Q}(i)|\mathbb{Q}}(\rho) < p$. Thus, ρ is a product of generators of the RHS with norm lower than p, then ρ belongs to the LHS by the starting assumption. Since also $c - i$ belongs to the LHS, equation A.1 allows us to conclude that also $(a \pm bi)$ does, contradicting the assumption. □

We now need to observe that $X^2 + 1$ is irreducible in $\mathbb{Q}_p[X]$ for primes $p \in I$.

Lemma A.2.3. *The polynomial $X^2 + 1$ is irreducible in $\mathbb{Q}_p[X]$ for every $p \equiv -1 \mod 4$.*

Proof. The polynomial $x^2 + 1$ is reducible in $\mathbb{Q}_p$ if and only if -1 admits a square root in $\mathbb{Q}_p$. By applying Hensel's Lemma we see that this is really equivalent to ask -1 to be a quadratic residue modulo p, i.e. there is $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$ and $a^2 \equiv -1 \bmod p$. Let p be odd: by the Fermat's Little Theorem we have

$$1 \equiv a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \bmod p.$$

Thus, $\frac{p-1}{2}$ must be even. So if $x^2 + 1$ is reducible in $\mathbb{Q}_p$ then $p = 2$ or $p \equiv 1 \bmod 4$. □

The following lemma implies all we are left to show.

Lemma A.2.4. *Let $\mathcal{S}$ be the set of elements of F^* satisfying condition (ii) in the Lenstra's Hypothesis, i.e. $\mathcal{S} := \{\beta \in F^* \mid \forall\ p \text{ integer prime} : \beta \hookrightarrow J_p \subseteq F_p^*\}$. Then*

$$\mathcal{S} = \langle i \rangle \times \langle 1 - i \rangle \times \langle a \pm bi \mid a^2 + b^2 = p \in S \rangle.$$

Proof. By Lemma A.2.2 the RHS is equal to J so the inclusion $\supseteq$ is trivial and we just need to prove that every element of $\mathcal{S}$ sits inside the RHS. By Lemma A.2.3 we have that

$$\forall\ p \in I : \quad \mathbb{Z}_p[i] = \mathbb{Z}_p \oplus i \cdot \mathbb{Z}_p$$

so given $p \in I$, an element $a + ib \in \mathbb{Z}_p[i]$ is divisible by $p \in I$ if and only if $p|a$ and $p|b$. Therefore, every element of the form $a - i$ for some $a \in \mathbb{Z}_p$ is invertible in $\mathbb{Z}_p[i]$, because it lies outside the maximal ideal $p \cdot \mathbb{Z}_p[i]$, so $J_p \subseteq (\mathbb{Z}_p[i])^*$. Then any element of F^* that is mapped inside J_p cannot have any factor $p \in I$, otherwise it would be mapped inside $p\mathbb{Z}_p[i]$; this proves inclusion $\subseteq$ and concludes the proof. □

Bibliography

[AKS02] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in P. *Ann. of Math*, 2:781–793, 2002.

[Art67] E. Artin. *Algebraic Numbers and Algebraic Functions.* AMS Chelsea Publishing Series. AMS Chelsea Pub./American Mathematical Society, 1967.

[CF67] J.W.S. Cassels and A. Fröhlich. *Algebraic number theory: proceedings of an instructional conference.* Thompson Book Co., 1967.

[Eis95] D. Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry.* Graduate Texts in Mathematics. Springer, 1995.

[Jac12] N. Jacobson. *Basic Algebra II: Second Edition.* Dover Books on Mathematics. Dover Publications, 2012.

[LL93] A.K. Lenstra and H.W. Lenstra. *The Development of the Number Field Sieve.* Number No. 1554 in Lecture Notes in Mathematics. Springer, 1993.

[LS91] H.W. Lenstra and P. Stevenhagen. Primes of degree one and algebraic cases of Čebotarev's theorem. *Enseign. Math.*, 37:17–30, 1991.

[Wei74] A. Weil. *Basic number theory.* Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1974.