Universiteit Utrecht

Master Thesis

# The Point Counting Function on Elliptic Curves

*Author:*
Koen van Woerden

*Supervisor:*
Prof. dr. Gunther Cornelissen

July 31, 2014

# Contents

# Introduction

Consider a scheme $X$ of finite type over $\mathbf{Z}$. For a rational prime $p$, denote by $N_X(p)$ the number of its $\mathbf{F}_p$-points, that is, the cardinality of $X(\mathbf{F}_p)$. More generally, if $q = p^e$, denote by $N_X(q)$ the number of its $\mathbf{F}_q$-points.

The goal of this thesis is to understand and prove in the case of elliptic curves the following

**Theorem (see part III theorem 8.1)** *Let $X, Y$ be two schemes of finite type over $\mathbf{Z}$. Assume that $N_X(p) = N_Y(p)$ for a set of primes of density 1. Then there exists a prime number $p_0$ such that $N_X(p^e) = N_Y(p^e)$ for all $p \geq p_0$ and all $e \geq 1$.*

from Serre [12, chap. 1, thm 1.3].

This theorem applies to elliptic curves, and one would expect that in proving the theorem only for the case of elliptic curves things would get eassier. This is indeed the case. The proof as given by Serre has two ingredients. Firstly the Lefschetz fixed point formula for cohomology, applied to the Frobenius acting on a variety of finite type over $\mathbf{Z}$. Secondly the Chebotarev density theorem. In this thesis a proof of theorem 8.1 in the case of elliptic curves is given in part III chapter 8, replacing the first ingredient by the trace of the Frobenius formula for the number of points on an elliptic curve, and leaving the second ingredient as it is.

In part II section 7.3 the trace formula for elliptic curves over finite fields is illustrated with two explicit examples, constructed using SAGE. The example illustrates that for a prime $\ell$, different from the characteristic of the finite field under consideration, the $\ell^m$-torsion group $E[\ell^m]$ is two dimensional $\mathbf{Z}/\ell^m\mathbf{Z}$-module. What is more, a basis of this module can be lifted to a basis of the $\ell^{m+1}$-torsion subgroup $E[\ell^{m+1}]$, and this in turn gives a lift of the matrix of the Frobenius involved. Taking the inverse limit, we see that we indeed get the number of points on $E$ in terms of the trace of the Frobenius acting on the Tate module $T_\ell(E)$ of $E$.

In part I the Chebotarev density theorem is treated using $L$-series and representation theory of Galois groups, which are developed starting from definitions. Also used is the Artin reciprocity law from Class Field Theory, which is stated without a proof.

Part II contains the relevant definitions and propositions on elliptic curves. For proofs of the latter we refer to Silverman [14], as well as for a thorough treatment of the subject.

Part III contains my proof of Serre's $N_X(p)$ theorem in the case of elliptic curves. We also deduce a corollary about weight-two newforms.

This thesis has two main parts: the proof of theorem 8.1 in the case of elliptic curves and a proof of Chebotarev's density theorem. The first can be found in part III chapter 8 and the second in part I chapter 5. Both chapters should be accessible to readers with the right background. In case of the proof of theorem 8.1 in the case of elliptic curves this background consists of properties of elliptic curves and Chebotarev's density theorem. In case of Chebotarev's density theorem this background consists of some representation theory of finite groups and properties of $L$-series defined on characters of Galois groups.

# Part I

# Preliminaries from algebraic number theory

# Introduction

We wish to say something about the number of points of two elliptic curves over all finite fields $\mathbf{F}_p$, for every rational prime $p$. To do so, we need the Chebotarev density theorem. The goal of this chapter is to state and prove that.

**Theorem (Chebotarev, see theorem 5.4)** *Let $K$ be a number field, $E$ a finite Galois extension of $K$ with Galois group $G$. For a place $v$ of $K$ that is unramified in $E$ let $\sigma_v$ be the conjugacy class of the generator of the decomposition group $D_w$ for any $w$ lying over $v$ (this is independent of $w$ because $v$ is unramified). Let $C$ be a subset of $G$ stable under inner automorphisms (a union of conjugacy classes). Let*

$$V_{K,C} = \{v \in V_K : v \textit{ is unramified and } \sigma_v \subset C\},$$

*then $V_{K,C}$ has a Dirichlet density (to be defined), and that density is equal to $\#C/\#G$.*

To prove this theorem we will follow the approach in Dokchitser [3].

To get an idea how the proof works before diving in all the preliminaries, it is useful to first read chapter 5, but skip the proof of proposition 5.3. Quite some terminology in the proof of theorem 5.4 may be unknown, but nonetheless it should be possible to get an idea how the proof works by reading it. Two things that might help to understand it at this stage are the following. The indicator function $C_{\mathcal{C}}$ is a class function on the Galois group, which means that it is constant on conjugacy classes and has values in $\mathbf{C}$. The $\mathbf{C}$-space of class functions has as an orthonormal basis (with respect to some scalar product (see remark 3.20)) the so called irreducible characters $\chi_\rho$. Given a character, we can define a function on the complex half plane $\mathrm{Re}(s) > 1$ by some series known as an $L$-series. With some work it can be shown that these $L$-series can be extended meromorphically to the half plane $\mathrm{Re}(s) > 1 - \epsilon$ for some suitable $\epsilon$, such that the resulting function is analytic everywhere except for a possible pole at $s = 1$. Moreover, only if the character was the so called trivial character the $L$-series will have a pole at $s = 1$, otherwise the $L$-series will be zero nor have a pole at $s = 1$.

Using the fact that the irreducible characters form an orthonormal basis, we decompose a certain series in that is defined in terms of $C$ as a sum over all the characters, and consider the trivial character separately, because its $L$-series has different asymptotic behaviour for $s \to 1$ than the other characters. Then we show that the two parts in fact behave as $L$ series times some constant. We divide by $\log(1/(s-1))$ which behaves asymptotically as the $L$-series for the trival character. Hence the part of $f(s)$ which corresponds to the non-trivial characters goes to zero in the limit of the quotient. What remains is the coefficient of the part corresponding to the trivial character, which is the sought density.

We made use of the asymptotic behaviour of the $L$-series of characters. They are obtained as follows. First we study the asymptotic behaviour of the number of prime ideals below a given norm of a number field when that norm goes to infinity. We apply this to show that we can extend the Riemann $\zeta$-function, which is a special case of an $L$-series. This is then applied to show that we can extend the $L$-series of characters of the ideal class group. After developing representation theory of Galois groups, the $L$-series for representations of Galois groups and the Artin formalism for these $L$-series, we apply Artin's reciprocity law to link the ideal class group to the Galois group and obtain that the $L$-series of the Galois representations can also be extended. This is then applied to the $L$-series of characters of the Galois group, because characters are in particular irreducible representations.

# Chapter 1

# Lattice Points in Homogeneously Expanding Domains

The material in this section comes from Lang [9, Chapter VI, §2]. To derive the asymptotic expression $j(\mathcal{R}, t)$ discussed in part I, we will use the geometry of numbers approach of associating to fractional ideals lattices in Euclidean space. We will then apply an asymptotic formula for the number of lattice points lying in certain domains, which will be derived in this section. Domain will just mean a certain well-behaved subset of Euclidean space.

Throughout the section, one can keep in mind the following special case. Let $L$ be the lattice (this notion is to be defined) in $\mathbf{R}^2$ generated as a $\mathbf{Z}$-module by the standard basis vectors: $L = \mathbf{Z}\begin{pmatrix}1\\0\end{pmatrix} + \mathbf{Z}\begin{pmatrix}0\\1\end{pmatrix}$. Let $D$ be a subset of $\mathbf{R}^2$ with a sufficiently regular boundary (made precise later). For example: $D = D^2 = \{(x,y) \mid \|(x,y)\| \leq 1\}$, the unit 2-disk. Let $t \in \mathbf{R}_{>0}$ and scale $D$ by a factor $t$. Count the number of lattice points in $tD$, that is, the number of points of $tD \cap L$. We will develop an asymptotic formula for this number of points as $t \to \infty$.

**Definition 1.1** A **lattice** in $\mathbf{R}^N$ is a discrete subgroup $L \subset \mathbf{R}^N$ of rank $N$. Since it is an abelian group it is a $\mathbf{Z}$-module, and by the rank we mean the rank as a $\mathbf{Z}$-module, that is, the number of elements of a $\mathbf{Z}$-basis of $L$. The next proposition shows that this number is well defined.

The following is from Lang [8, Chapter XV, §2]

**Proposition 1.2** *Let $M$ be a free module over a principal ideal domain $A$. Then the cardinality of an $A$-basis is uniquely determined.*

PROOF Suppose $A$ has no irreducibles. Then by unique factorization, $A$ is a field. Hence $M$ is a vector space. The $A$-rank is then equal to the $A$-dimension, which is uniquely detrmined.

Suppose $A$ has an irreducible, $p$ say. Then $(p)$ is a maximal ideal. Then $M/pM$ is an $A/pA$ vector space whose dimension is the rank of $M$, which is therefore uniquely determined. ■

We now show that a **Z**-basis of a lattice is always an **R**-linearly independent set. This, and a little more, is the content of the next proposition, which is from Knapp [7, Chapter 5, section 5].

**Proposition 1.3** *Let $L \subset \mathbf{R}^N$ be a discrete subgroup in the induced topology (not necessarily of rank $N$). Then $L$ is a free group of rank $\leq N$. Furthermore, $L$ is of the form*

$$L = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_m,$$

*with the $\omega_1, \ldots, \omega_m$ **R**-independent. The number $m$ is the dimension of the **R**-span of $L$. The sum is in fact direct, hence $L \cong \mathbf{Z}\omega_1 \oplus \cdots \oplus \mathbf{Z}\omega_m$.*

PROOF We first show that $L$ is a closed set. Since $L$ is discrete, there is an $\epsilon > 0$ such that $B(0;\epsilon) \cap L = \{0\}$. Suppose $x_0$ is a limit point of $L$ that is not in $L$. Then $x_0 - B(0;\epsilon/2)$ (the sphere with radius $\epsilon/2$ around $x_0$) contains a point of $L$, $l$ say. Write $b = x_0 - l \in B(0;\epsilon/2)$. Then $b \notin L$, for else $x_0 \in L$. Furthermore, $b$ is a limit point of $L$. Otherwise, there would be an open $U$ around $b$ with $U \cap L = \varnothing$. This would give $U + l \cap L = \varnothing$, but $U + l$ is an open containing $x_0$, so this cannot happen since $x_0$ is a limit point of $L$. Hence $b + B(0; \min(\epsilon/2, \|b\|)) \cap L \neq \varnothing$, hence it contains an element, $l'$ say. Then $l' \neq 0$. Furthermore,

$$\begin{aligned} d(l', 0) &\leq d(l', b) + d(b, 0) \\ &< \epsilon/2 + \epsilon/2 \\ &= \epsilon. \end{aligned}$$

Hence $0 \neq l' \in B(0;\epsilon)$, a contradiction. Hence $L$ is closed.

Since $L$ is closed, every bounded subset of $L$ is compact, hence finite since $L$ is discrete.

Let $m$ be the dimension of the **R**-linear span of $L$. We use induction on $m$. First consider the case $m = 1$. The set $B(0;1) \cap L$ is finite. Let $\omega$ be an element of smallest norm in this set. Suppose there is a $v \in L$ that is not an integral multiple of $\omega$. Then there exists a $j \in \mathbf{Z}$ such that $v - j\omega$ is of norm smaller than $\omega$, a contradiction. Hence every $v \in L$ is an integral multiple of $\omega$, and the base case is established.

Now assume that the proposition holds if the dimension is $m - 1$. Let $L$ be such that the dimension of its **R**-span is $m$. Let $\{x_1, \ldots, x_m\}$ be an **R**-basis for this **R**-span. Then $L_0 := L \cap (\sum_{j=1}^{m-1} \mathbf{R}x_j)$ is a discrete subgroup of $\mathbf{R}^N$, and its $\mathbf{R}$-span is $m-1$ dimensional. By induction $L_0$ is generated as a $\mathbf{Z}$-module by some $\omega_1, \ldots, \omega_{m-1}$ which are $\mathbf{R}$-linearly independent. Consider the set

$$S = L \cap \{c_1\omega_1 + \ldots c_{m-1}\omega_{m-1} + c_m x_m \ \mid 0 \leq c_i \leq 1\}.$$

Then $S$ is a bounded subset of $L$, hence finite. Note that $\omega_1, \ldots, \omega_{m-1}, x_m$ are linearly independent, hence the coefficients $c_i$ of elements in $S$ are uniquely determined. Also note that $S$ contains the element $x_m$ which has a non-zero $x_m$-coefficient. Hence by finiteness of $S$, there is a $\omega_m \in S$ with smallest non-zero $x_m$ coefficient, $a_m$ say. Let $v \in S$. Suppose its $x_m$-coefficient is not an integral multiple of $a_m$. Then $v - j\omega_m$ for a suitable $j \in \mathbf{Z}$ has an $x_m$-coefficient smaller than $a_m$, and after subtracting suitable $\mathbf{Z}$-multiples of the $\omega_1, \ldots, \omega_{m-1}$ we get an element of $S$ with $x_m$ coefficient smaller than $a_m$, a contradiction.

Let $l \in L$. Then $l$ is a linear combination of the $\omega_1, \ldots, \omega_{m-1}, x_m$. After subtracting suitable integral multiples of these elements we get an element in $S$, $l'$ say. As we just saw, for a suitable $j \in \mathbf{Z}$ we have $l' - j\omega_m \in L \cap (\sum_{j=1}^{m-1} \mathbf{R}x_j)$. Hence

$$\begin{aligned} L &= L \cap (\sum_{j=1}^{m-1} \mathbf{R}x_j) + \mathbf{Z}\omega_m \\ &= (\mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_{m-1}) + \mathbf{Z}\omega_m \\ &\cong (\mathbf{Z}\omega_1 \oplus \cdots \oplus \mathbf{Z}\omega_{m-1}) + \mathbf{Z}\omega_m \end{aligned}$$

The elements $\omega_1, \ldots, \omega_{m-1}, \omega_m$ are linearly independent because by assumption the first $m-1$ are and the last is the only one with non-zero $x_m$-coefficient. Hence the intersection of the two summands is empty and the sum is direct:

$$L \cong \mathbf{Z}\omega_1 \oplus \cdots \oplus \mathbf{Z}\omega_{m-1} \oplus \mathbf{Z}\omega_m$$

This completes the induction. ∎

**Corollary 1.4** *A lattice in $\mathbf{R}^N$ is generated by $N$ linearly independent elements as a $\mathbf{Z}$-module. A lattice is maximal in the sense that there are no discrete subgroups of higher rank strictly containing it. Every $\mathbf{Z}$-basis of a discrete subgroup of $\mathbf{R}^N$ consists of $\mathbf{R}$-linearly independent elements, in particular any $\mathbf{Z}$-basis of a lattice consists of such elements.*

Proof The first two statements follow immediately from proposition 1.3.

For the third statement, let $L \subset \mathbf{R}^N$ be a discrete subgroup. From the proof op proposition 1.3, the rank of $L$ is the dimension of the $\mathbf{R}$-linear span of $L$, $m$ say. By proposition 1.3, we can find an $\mathbf{R}$-independent set $\omega_1, \ldots, \omega_m$ that $\mathbf{Z}$-generates $L$. Every other $\mathbf{Z}$-basis of $L$ has the same cardinality by proposition 1.2. Let $\mu_1, \ldots, \mu_m$ be such a $\mathbf{Z}$-basis. Let $A$ be the $m \times m$ matrix with respect to the basis $\omega_1, \ldots, \omega_m$ in the domain and the codomain that describes the $\mathbf{Z}$-linear map that sends $\omega_i$ to $\mu_i$. Since both $\{\omega_i\}_i$ and $\{\mu_i\}_i$ are $\mathbf{Z}$-bases, also the inverse matrix $A^{-1}$ exists and has coefficients in $\mathbf{Z}$. But this implies that $\mathbf{R}$-linear map that $A$ also represents, going from $\mathbf{R}\omega_1 + \cdots + \mathbf{R}\omega_m$ to $\mathbf{R}\mu_1 + \cdots + \mathbf{R}\mu_m$ is a linear isomorphism, hence the $\{\mu_i\}_i$ are linearly independent.

The last statement follows immediately from the third. ■

We will study lattice points in expanding sets, whence the following definition.

**Definition 1.5** Let $D \subset \mathbf{R}^N$. By $\partial D$ we denote the boundary of $D$. For $t \in \mathbf{R}$, $tD$ is the set of points $tx$ with $x \in D$.

**Proposition 1.6** *Situation as in definition 1.5. Then* $\partial(tD) = t(\partial D)$.

Proof In the case $t \neq 0$ multiplication by $t$ is a homeomorphism, which gives the desired equality. If $t = 0$ both sides become $\{0\}$ so that's also alright. ■

To get to an asymptotic estimation we will need a regularity condition on the boundary of the expanding set under consideration. That condition is given by the following two definitions.

**Definition 1.7** Let $S$ be a subset of some Euclidean space. A map

$$\varphi\colon S \to \mathbf{R}^N$$

is said to satisfy a **Lipschitz condition** if there exists a $C > 0$ such that for all $x, y \in S$ we have

$$\|\varphi(x) - \varphi(y)\| \leq C\|x - y\|$$

**Definition 1.8** Let $I^k$ denote the unit cube in Euclidean $k$-space. A subset $T \subset \mathbf{R}^N$ is said to be **$k$-Lipschitz parametrizable** if there exists a finite number of Lipschitz maps $\varphi_j\colon I^k \to T$ where the images of the $\varphi_j$ cover $T$. .

**Definition 1.9** Let $L$ be a lattice in $\mathbf{R}^N$, and let $\omega_1, \ldots, \omega_N$ be a basis of $L$. Then the set $F$ all all points

$$t_1\omega_1 + \cdots + t_N\omega_N \quad (0 \leq t_i < 1),$$

will be called a **fundamental domain** of $L$.

**Proposition 1.10** *Situation as in definition 1.9. The translations $F_l := l + F$ with $l \in L$ cover $\mathbf{R}^N$ and are disjoint. Every element in $\mathbf{R}^N$ has a unique representative in $F$ modulo $L$. Let* Vol *denote the volume in $N$-space. Then* Vol$(F)$ *only depends on the lattice $L$, hence is independent of the choice of fundamental domain $F$.*

Proof Let $v \in \mathbf{R}^N$. There is a unique lattice point $l \in L$ such that $v - l \in F$, since all the $t_i$ satisfy $0 \leq t_i < 1$. Then $v \in l + F = F_l$. Hence the $F_l$ cover $\mathbf{R}^N$, and since the $F_l$ covering $v$ was unique the $F_l$ are pairwise disjoint.

As in the proof of corollary 1.4 we let $\{\mu_i\}_i$ be another $\mathbf{Z}$-basis of $L$, and let $F'$ be the corresponding fundamental domain. The $N \times N$ matrix $A$ with respect to the basis $\{\omega_i\}_i$ in the domain and the codomain representing the **Z**-linear map that sends $\omega_i$ to $\mu_i$ is invertible. Hence $\det(A)\det(A^{-1}) = \det(AA^{-1}) = \det(I) = 1$. But note that $A$ and $A^{-1}$ are matrices with entries in $\mathbf{Z}$. Hence both determinants are integers with product 1, hence they are ±1. Therefore

$$\begin{aligned}\mathrm{Vol}(F') &= \mathrm{Vol}(AF)\\ &= |\det(A)|\,\mathrm{Vol}(F)\\ &= \mathrm{Vol}(F).\end{aligned}$$

■

**Proposition 1.11** *Let $L \subset \mathbf{R}^N$ be a lattice, $R > 0$. There is a $K > 0$ such that for every set $S$ of diameter $\leq R$ the number of $l \in L \cap S$ is bounded by $K$.*

Proof Let $\{\omega_i\}_i$ be a **Z**-basis for $L$. Let $\|\cdot\|_\omega$ denote the sup-norm with respect to this basis:

$$\|\lambda_1\omega_1 \cdots + \lambda_N\omega_N\|_\omega = \sup_i |\lambda_i|.$$

Since all norms on $\mathbf{R}^N$ are equivalent, there exists a $C > 0$ such that $\|x\|_\omega \leq C\|x\|$ for all $\in \mathbf{R}^N$, where the second norm is the euclidean one. Let $S$ be of diameter $\leq R$. Let $l \in S \cap L$. For every $l' \in S \cap L$ we have

$$\begin{aligned}\|l - l'\|_\omega &\leq C\|l - l'\|\\ &\leq CR,\end{aligned}$$

hence the $\omega_i$-coordinates of $l'$ are bounded, hence the number of points $l'$ is bounded by $(2CR)^N$. ■

**Proposition 1.12** *Let $L \subset \mathbf{R}^N$ be a lattice, $F$ a fundamental domain of $L$, $R > 0$. There is a $K > 0$ such that for every set $S$ of diameter $\leq R$ the number of $l \in L$ such that $F_l \cap S \neq \varnothing$ is bounded by $K$.*

Proof Let $\|\cdot\|_\omega$ be as in the proof of proposition 1.11. Since $F$ has a finite diameter with respect to the $\|\cdot\|_\omega$-norm, it also has a finite diameter with respect to the Euclidean norm. Let $l \in L$ be such that $F_l \cap S \neq \varnothing$. Let $l' \in L$ also be such that $F_{l'} \cap S \neq \varnothing$. Then $d(l, l') \leq \mathrm{Diam}(F) + \mathrm{Diam}(S) + \mathrm{Diam}(F)$, hence the number of such $l'$ is bounded by a constant that depends only on $L$ and $\mathrm{Diam}(S)$. ■

**Definition 1.13** A **translated lattice** $T$ is a set in $\mathbf{R}^N$ of the form $x + L$ with $x \in \mathbf{R}^N$ and $L \subset \mathbf{R}^N$ a lattice. If $F$ is a fundamental domain of $L$ then $x + F$ will also be called a **fundamental domain** of $T$.

**Proposition 1.14** *Let $T = x + L \subset \mathbf{R}^N$ be a translated lattice, $x + F$ a fundamental domain of $T$, $R > 0$. There is a $K > 0$ such that for every set $S$ of diameter $\leq R$ the number of $l \in L$ such that $(x + F)_l \cap S \neq \varnothing$ is bounded by $K$.*

Proof The proof is the same as that of proposition 1.12. Notice that in that proof the important thing was that $\mathrm{Diam}(F)$ was bounded, but $\mathrm{Diam}(x+F) = \mathrm{Diam}(F)$ so that still works. ■

We are now ready to prove the asymptotic formula we need for the number of lattice points in expanding domains. Keep in mind the example at the beginning of this subsection for intuition.

**Theorem 1.15** *Let $L \subset \mathbf{R}^N$ be a lattice, $D \subset \mathbf{R}^N$ such that $\partial D$ is $(N-1)$-Lipschitz parametrizable and* $\mathrm{Vol}(D)$ *is finite. Let $F$ be a fundamental domain of $L$. Let $\lambda(t, D, L) = \lambda(t) = \#(L \cap tD)$. Then*

$$\lambda(t) = \frac{\mathrm{Vol}(D)}{\mathrm{Vol}(F)} t^N + O(t^{N-1})$$

*where the constant in $O$ depends on $L, N$ and the Lipschitz constants.*

**Remark 1.16** The intuition is that the first term corresponds to the points in the interior of $D$, which grows like $t^N$, and the second term corresponds to the number of points on the boundary, which is of one "dimension" lower and hence grows like $t^{N-1}$.

**Remark 1.17** The Lipschitzparametrizability of the boundary is really necessary, as the following non-example shows.

Take $L = \mathbf{Z} \subset \mathbf{R}$, $D = (-1, 1) \setminus \mathbf{Q}$. If Theorem 1.15 would hold for $\lambda(t)$ in this case, then $\lambda(t)$ would grow linearly: we have $\mathrm{Vol}(D) = 1$, $\mathrm{Vol}(F) = 1$. Hence in that case we would get

$$\lambda(t) = t + O(t^0).$$

But note that

$$\partial D = [-1, 1] \setminus \varnothing = [-1, 1],$$

and $[-1, 1]$ is not 0-Lipschitz Parametrizable, since $I^0$ is just a point an $[-1, 1]$ contains an infinite number of points.

If theorem 1.15 would hold then there would be some $C > 0$ such that

$$|\lambda(t) - t| < C$$

for all $t$ large enough. But note that for all rational $t$, $\lambda(t) = 0$. Take $t > C$ rational to see that theorem 1.15 does not hold.

Proof (of theorem 1.15) Define

$$m(t) = \#\{l \in L \mid F_l \subset \mathrm{Int}(tD)\},$$
$$b(t) = \#\{l \in L \mid F_l \cap \partial tD \neq \varnothing\}.$$

Then

$$\{l \in L \mid F_l \subset \mathrm{Int}(tD)\} \subset L \cap tD \subset (L \cap tD) \cup \{l \in L \mid F_l \cap \partial tD \neq \varnothing\},$$

hence

$$m(t) \leq \lambda(t) \leq m(t) + b(t).$$

Regarding $\mathrm{Vol}(tD)$, we can make the following two observations. First, we can estimate $\mathrm{Vol}(tD)$ from below by counting how many of the $F_l$ are completely contained in $\mathrm{Int}(tD) \subset tD$, and then multiply this number by $\mathrm{Vol}(F)$ (since $\mathrm{Vol}(F_l) = \mathrm{Vol}(F)$ for every $l$ and all the $F_l$ are pairwise disjoint). This gives:

$$m(t) \, \mathrm{Vol}(F) \leq \mathrm{Vol}(tD).$$

The second observation is that for every $l \in L$ exactly one of the following three holds:

- $F_l \subset \mathrm{Int}(tD)$,
- $F_l \subset \mathbf{R}^N \setminus \overline{tD}$,
- $F_l \cap \partial(tD) \neq \varnothing$.

To see this, note that the first two are mutually exclusive. Suppose that the first two do not hold. Then $F_l$ is not contained in $(\overline{tD})^c$ (here the $c$ superscript denotes complement in $\mathbf{R}^N$), hence it has points in $(\overline{tD})^c$. Also $F_l$ is not contained in $\mathrm{Int}(tD)$, hence it has also points in there. Suppose $F_l$ has no points on the boundary $\partial(tD)$. Then $F_l$ would be equal to the disjoint union of non-empty opens $(F_l \cap \mathrm{Int}(tD)) \cup (F_l \cap (\overline{tD})^c)$, contradicting the connectedness of $F_l$.

Now the $F_l$ satisfying the first and last condition cover $tD$, hence we get the inequality

$$\mathrm{Vol}(tD) \leq (m(t) + b(t)) \, \mathrm{Vol}(F)$$

Combining these two inequalities gives

$$m(t) \, \mathrm{Vol}(F) \leq \mathrm{Vol}(tD) \leq (m(t) + b(t)) \, \mathrm{Vol}(F),$$

hence

$$m(t) \leq \frac{\mathrm{Vol}(D)}{\mathrm{Vol}(F)} t^N \leq m(t) + b(t),$$

therefore $|\lambda(t) - \frac{\mathrm{Vol}(D)}{\mathrm{Vol}(F)} t^N| \leq b(t)$. Hence a good enough estimation of $b(t)$, of order $O(t^{N-1})$ that is, would give the desired result.

Consider a finite set of Lipschitz maps parametrizing $\partial D$, and let $C$ be the maximum of their Lipschitz constants. Let $\varphi\colon I^{N-1} \to \mathbf{R}^N$ be one of the parametrizing maps for a piece of $\partial D$. Then $t\varphi$ parametrizes a corresponding piece of $\partial tD$. Cut up each side of the unit $I^{N-1}$ cube into sides of length $1/\lceil t \rceil$ (since we want an asymptotic formula for $t \to \infty$ we can asume that $t > 0$). We then get $\lceil t \rceil^{N-1}$ small cubes. The image of each small cube under $\varphi$ has a diameter $\leq C/\lceil t \rceil$. Hence the image of each small cube under $t\varphi$ has diameter

$\leq C$. By proposition 1.12 there is a $K > 0$ such that for every set $S$ of diameter $\leq C$ there are $\leq K$ lattice points such that $F_l \cap S \neq \varnothing$. Hence the number of lattice points $l$ such that $F_l$ intersects the image $t\varphi[I^{N-1}]$ is $\leq K\lceil t\rceil^{N-1}$, as we divided $I^{N-1}$ into $\lceil t\rceil^{N-1}$ small cubes. There are a finite number of parametrizing maps, $M$ say. Hence the total number of points intersecting any one of the images is bounded by $MK\lceil t\rceil^{N-1}$. This gives an upper bound for $b(t)$:

$$\begin{aligned} b(t) &\leq MK\lceil t\rceil^{N-1} \\ &\leq MK(t+1)^{N-1} \\ &\leq 2MKt^{N-1} \end{aligned}$$

. ■

This result can be extended to translated lattices.

**Theorem 1.18** *Let $T = x + L \subset \mathbf{R}^N$ be a translated lattice, $D \subset \mathbf{R}^N$ such that $\partial D$ is $(N-1)$-Lipschitz parametrizable. Let $x + F$ be a fundamental domain of $L$. Let $\lambda(t, D, T) = \lambda(t) = \#(T \cap tD)$. Then*

$$\lambda(t) = \frac{\text{Vol}(D)}{\text{Vol}(F)} t^N + O(t^{N-1})$$

*where the constant in $O$ depends on $T, N$ and the Lipschitz constants.*

Proof All our formulas in the proof of theorem 1.15 still work. To estimate $b(t)$ we used proposition 1.12. Use in this case proposition 1.14 instead. ■

# Chapter 2

# Asymptotic Behaviour of the Number of Integral Ideals of Bounded Norm going to Infinity

## 2.1 Generalized ideal classes

The material in this section comes from Lang [9, Chapter VI, §1].

A special case of the asymptotic formula that we need is given by the following. Let $K$ be a number field, $\mathcal{O}$ its ring of integers, $I$ its group of fractional ideals of $\mathcal{O}$, $P \lhd I$ the subgroup of principal fractional ideals, $\mathrm{Cl}_K = I/P$ the ideal class group of $K$. For a fractional ideal $\mathfrak{a}$ denote by $\mathbf{N}\mathfrak{a}$ its norm. That is, for prime ideals $\mathfrak{p}$ we have $\mathbf{N}\mathfrak{p} = \#\mathcal{O}/\mathfrak{p}$. This is then extended multiplicatively to all of $I$, which is a free group on the prime ideals. Let $\mathcal{R}$ be an element of $\mathrm{Cl}_K$. Denote by $j(\mathcal{R}, t)$ the number of integral ideals $\mathfrak{a}$ in the class $\mathcal{R}$ of norm $\mathbf{N}\mathfrak{a} \leq t$. Then, as we shall see in section 2.3, $j(\mathcal{R}, t)$ exhibits the following asymptotic behaviour in $t$:

$$j(\mathcal{R}, t) = pt + O(t^{1-[K:\mathbf{Q}]}), \qquad t \to \infty, \tag{2.1}$$

where $p$ is some constant depending on $K$ but not on $\mathcal{R}$.

We will need such a statement in section 4.1 to show that we can extend certain functions considered there, by analytic continuation. For that goal, eq. (2.1) is not sufficient, for we will consider extensions of number fields. When we do that, we need to exclude ramifying primes. Therefore we need a version of eq. (2.1) which allows us to do this. We need a way to specify primes that we wish to exclude. That is accomplished by the following concept.

**Definition 2.1** Let $K$ be a number field. By a **cycle** (of $K$) we mean a formal product

$$\mathfrak{c} = \prod_{v \in M_K} v^{m(v)},$$

where $v$ ranges over $M_K$, the normalized absolute values of $K$ (which means for the finite ones that they restrict to a $p$-adic absolute value on $\mathbf{Q}$), with $m(v) \in \mathbf{Z}_{\geq 0}$ and $m(v) = 0$ for all but finitely many $v$. We do not care about the complex $v$, and when $v$ is real we only care whether $m(v) = 0$ or $m(v) > 0$, hence we can take $m(v) \in \{0, 1\}$ for real $v$. If $m(v) > 0$ we say that $v$ **divides** $\mathfrak{c}$. We call $m(v)$ the multiplicity of $v$ in $\mathfrak{c}$. We denote by

$$\mathfrak{c}_v = v^{m(v)}$$

the **local $v$-component**, and if $v$ corresponds to a prime $\mathfrak{p}$ also denote

$$\mathfrak{c}_\mathfrak{p} = \mathfrak{p}^{m(v)}.$$

We denote by

$$\mathfrak{c}_0 = \prod_{v \text{ finite}} v^{m(v)}$$

the **finite part** of $\mathfrak{c}$.

We wish to be able to exclude a finite set of prime ideals from consideration. Hence the following definition.

**Definition 2.2** Let $K$ be a number field, $\mathfrak{c}$ a cycle, $I$ the group of ideals. Then $I(\mathfrak{c})$, $I(K, \mathfrak{c})$ and $I_K(\mathfrak{c})$ all denote the subgroup of the group of ideals generated by the finite primes $\mathfrak{p}$ that do not divide $\mathfrak{c}$. Hence it consists of all fractional ideals $\frac{\mathfrak{a}}{\mathfrak{b}}$ with $\mathfrak{a}$ and $\mathfrak{b}$ integral such that for every finite prime $\mathfrak{p}|\mathfrak{c}$ we have $\mathfrak{p} \nmid \mathfrak{a}$ and $\mathfrak{p} \nmid \mathfrak{b}$. We call this group the **$\mathfrak{c}$-class group**.

In definition 2.2 we have generalized the notion of the ideal group so that we can exclude a finite set of primes. We wish to also generalize the notion of the ideal class group. For that it is not enough to look simply at the principal prime ideals that are in $I(\mathfrak{c})$, we need a little more.

**Definition 2.3** Let $K$ be an number field, $\mathfrak{c}$ a cycle, $\alpha \in K$. Define $\alpha \equiv 1$ (mod* $\mathfrak{c}$) to mean the following:

(i) If $\mathfrak{p}$ divides $\mathfrak{c}$ with multiplicity $m(\mathfrak{p}) > 0$, then $\alpha$ lies in the local ring $\mathcal{O}_\mathfrak{p}$, and

$$\alpha \equiv 1 \pmod{\mathfrak{m}_\mathfrak{p}},$$

where $\mathfrak{m}_\mathfrak{p}$ is the maximal ideal of $\mathcal{O}_\mathfrak{p}$. We also write for this

$$\alpha \equiv 1 \quad (\text{mod}^* \ \mathfrak{c}_\mathfrak{p}).$$

(ii) If $v$ is a real absolute value dividing $\mathfrak{c}$, and $\sigma_v$ is the corresponding embedding in $\mathbf{R}$, then

$$\sigma_v \alpha > 0.$$

Definition 2.3 allows us to define the group of principal ideals that we need.

**Proposition 2.4** *Let $K$ be a number field, $\mathfrak{c}$ be a non-empty cycle (hence divisible by some prime of $K$). Then the set of elements of $K^*$ that satisfy (i) and (ii) of definition 2.3 form a multiplicative subgroup of $K$. We denote this group by $K_\mathfrak{c}$. The elements of this group $K_\mathfrak{c}$ are $\mathfrak{p}$-units for $\mathfrak{p}|\mathfrak{c}$.*

Proof We first show that $0 \notin K_\mathfrak{c}$. Suppose $\mathfrak{c}$ is divisible by some finite prime $\mathfrak{p}$. Then by (i) we would have for $\alpha = 0$ that $0 \equiv 1 \pmod{\mathfrak{m}^{m(\mathfrak{p})}}$, hence that $1 \in \mathfrak{m}^{m(\mathfrak{p})}$, hence that $\mathfrak{m}^{m(\mathfrak{p})} = \mathcal{O}_\mathfrak{p}$, a contradiction. Suppose that $\mathfrak{c}$ is divisible by some real prime $v$. Then $\sigma_v 0 > 0$ cannot hold. Since $\mathfrak{c}$ is non-empty, one of the two previous cases holds. Hence $0 \notin K_\mathfrak{c}$.

We now verify that $K_\mathfrak{c}$ is closed under products and inverses. Let $\mathfrak{p}$ and $v$ be finite and real primes respectively dividing $\mathfrak{c}$. Let $\alpha, \beta \in K_\mathfrak{c}$. Then $\alpha, \beta \in \mathcal{O}_\mathfrak{p}$, hence $\alpha = a/s, \beta = b/t$, with $a, b \in \mathcal{O}$ and $s, t \notin \mathfrak{p}$. Then $\alpha\beta = ab/(ts)$, and $ab \in \mathcal{O}$ and $ts \notin \mathfrak{p}$ since $\mathfrak{p}$ is prime. Of course we also have $\alpha\beta \equiv 1 \cdot 1 = 1 \pmod{\mathfrak{m}^{m(\mathfrak{p})}}$ Concerning the real primes we have $\sigma_v\alpha > 0$ and $\sigma_v\beta > 0$, hence $\sigma_v\alpha\beta = \sigma_v\alpha\sigma_v\beta > 0$. Hence $K_\mathfrak{c}$ is closed under multiplication.

We also need to check that $K_\mathfrak{c}$ contains the inverses of its elements. Let $\alpha \in K_\mathfrak{c}$. Then $\alpha = a/s$ with some $a \in \mathcal{O}$ and $s \notin \mathfrak{p}$. Then we must verify that $\alpha^{-1} = s/a$ also satisfies (i) and (ii). To this end, we will show that $\alpha \notin \mathfrak{p}$. Suppose that $\alpha \in \mathfrak{p}$. Then $s\alpha \in \mathfrak{m}_\mathfrak{p}$. Hence $s \in \mathfrak{m}_\mathfrak{p}$ or $\alpha \in \mathfrak{m}_\mathfrak{p}$, but the second option is impossible since $\alpha \equiv 1 \pmod{\mathfrak{m}^{m(\mathfrak{p})}}$. Now, $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}\mathcal{O}_\mathfrak{p}$. Hence this implies that there is a $\lambda \in \mathfrak{p}$ and a $\mu \notin \mathfrak{p}$ such that $s = \lambda/mu$, hence that $s\mu = \lambda \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime this implies that $s \in \mathfrak{p}$ or $\mu \in \mathfrak{p}$, but as the second option does not hold the first option must hold. But the second option also does not hold. Hence $a \notin \mathfrak{p}$, and $\alpha^{-1}$ lies in the local ring $\mathcal{O}_\mathfrak{p}$ at $\mathfrak{p}$.

Of course, for a real embedding we have $\sigma_v\alpha^{-1} = 1/\sigma_v\alpha > 0$. Hence $K_\mathfrak{c}$ is closed under inverses.

Hence $K_\mathfrak{c}$ is indeed a group. In the proof we saw that if $\alpha = a/s \in K_\mathfrak{c}$ with $a \in \mathcal{O}$ and $s \notin \mathfrak{p}$ that then also $a \notin \mathfrak{p}$, hence $\alpha$ is indeed a $\mathfrak{p}$-unit. ■

**Definition 2.5** Let $K$ be a number field, $\mathfrak{c}$ a cycle. Then $P_\mathfrak{c}$ is the set of principal ideals $(\alpha)$ with $\alpha \in K_\mathfrak{c}$.

**Proposition 2.6** *The set $P_\mathfrak{c}$ from definition 2.5 is a group. It is a subgroup of $I(\mathfrak{c})$.*

Proof That $P_\mathfrak{c}$ is a group follows immediately from the fact that $K_\mathfrak{c}$ is a group, which was shown in proposition 2.4.

Let $\alpha \in K_\mathfrak{c}$. We wish to show that $(\alpha) = \alpha\mathcal{O} \in I(\mathfrak{c})$. Let $\mathfrak{p}|\mathfrak{c}$. Since $\alpha$ is a $\mathfrak{p}$-unit, the localization of this ideal is $(\alpha\mathcal{O}) = \mathcal{O}_\mathfrak{p}$. Note that by localizing at

$\mathfrak{p}$, every prime ideal distinct from $\mathfrak{p}$ gets mapped to $\mathcal{O}_{\mathfrak{p}}$, and the ideal $\mathfrak{p}$ gets mapped to $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$. Consider the factorization with numerator and denominator relatively prime:

$$\alpha\mathcal{O} = \frac{\mathfrak{p}_1^{e(\mathfrak{p}_1)} \cdots \mathfrak{p}_i^{e(\mathfrak{p}_i)} \cdots \mathfrak{p}_s^{e(\mathfrak{p}_s)}}{\mathfrak{q}_1^{e(\mathfrak{q}_1)} \cdots \mathfrak{q}_j^{e(\mathfrak{q}_j)} \cdots \mathfrak{q}_r^{e(\mathfrak{q}_r)}}$$

with all exponents $e(\mathfrak{p}_i), e(\mathfrak{q}_j)$ non-zero. Localization at a prime $\mathfrak{p}$ is a group homomorphism from the fractional ideals of $\mathcal{O}$ onto the fractional ideals of the local ring $\mathcal{O}_{\mathfrak{p}}$ . The kernel consists of the ideals that meet $\mathcal{O} - \mathfrak{p}$. Suppose $\mathfrak{p}|\mathfrak{p}_i$. This would imply $\mathfrak{p} = \mathfrak{p}_j$ and hence $(\alpha\mathcal{O})_{\mathfrak{p}} = \mathfrak{p}^{e(\mathfrak{p}_i)}\mathcal{O}_{\mathfrak{p}}$, a contradiction. Suppose $\mathfrak{p}|\mathfrak{q}_j$. This would imply $\mathfrak{p} = \mathfrak{q}_j$ and hence $(\alpha\mathcal{O})_{\mathfrak{p}} = \mathfrak{p}^{-e(\mathfrak{q}_j)}\mathcal{O}_{\mathfrak{p}}$, a contradiction. Hence $\alpha\mathcal{O} \in I(\mathfrak{c})$. ■

**Definition 2.7** Let $X$ be a set, $\mathfrak{c}$ a cycle. Whenever it makes sense we denote by $X(\mathfrak{c})$ the subset of elements of $X$ prime to $\mathfrak{c}$ and by $X_{\mathfrak{c}}$ the subset of $X$ of elements satisfying (i) and (ii) of definition 2.3.

**Proposition 2.8** *Every class in $I/P$ has a representative in $I(\mathfrak{c})/P(\mathfrak{c})$.*

Proof Let $\mathfrak{a}$ (mod $P$) $\in I/P$. For a prime $\mathfrak{p}$ let $\pi_{\mathfrak{p}}$ denote an element of order 1 at $\mathfrak{p}$. Use the Chinese Remainder Theorem to find an $\alpha \in \mathcal{O}_k$ such that

$$\alpha \equiv \pi_{\mathfrak{p}}^{\operatorname{ord}_{\mathfrak{p}} \mathfrak{a}} \pmod{\mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})+1}}$$

for all $\mathfrak{p}|\mathfrak{c}$. Then $\mathfrak{a}\alpha^{-1}$ is prime to $\mathfrak{c}$. By the proof of proposition 2.17 we can multiply $\mathfrak{a}\alpha^{-1}$ by an integer to make it an integral ideal. ■

Thus

$$\begin{tikzcd}
I(\mathfrak{c}) \arrow[r, hook] \arrow[d, dash] & I \arrow[d, dash] \\
P \cap I(\mathfrak{c}) \arrow[r, hook] & P
\end{tikzcd}$$

induces an isomorphism

$$I(\mathfrak{c})/P(\mathfrak{c}) \cong I/P,$$

where $P(\mathfrak{c}) = P \cap I(\mathfrak{c})$.

Note that we have a tower

$$I(\mathfrak{c}) \supset P(\mathfrak{c}) \supset P_{\mathfrak{c}}.$$

Therefore we have a surjective homomorphism

$$I(\mathfrak{c})/P_{\mathfrak{c}} \twoheadrightarrow I(\mathfrak{c})/P(\mathfrak{c}) \cong I/P$$

with kernel $P(\mathfrak{c})/P_{\mathfrak{c}}$. We will now analyse this kernel.

Consider the map

$$\begin{aligned} k^* &\twoheadrightarrow P, \\ \alpha &\mapsto (\alpha). \end{aligned}$$

The kernel of this map is the group of units $U$. The inverse image of $P_{\mathfrak{c}} \subset P$ is $Uk_{\mathfrak{c}}$ (Recall: $P_{\mathfrak{c}}$ is by defnition $\{(\alpha)\colon \alpha \in k_{\mathfrak{c}}\}$.) Hence we have

$$\begin{tikzcd} k(\mathfrak{c}) \arrow[r, two heads] \arrow[d, dash] & P(\mathfrak{c}) \arrow[d, dash] \\ Uk_{\mathfrak{c}} \arrow[r, two heads] & P_{\mathfrak{c}} \end{tikzcd},$$

and therefore we have an isomorphism

$$k(\mathfrak{c})/Uk_{\mathfrak{c}} \xrightarrow{\sim} P(\mathfrak{c})/P_{\mathfrak{c}}.$$

Let $\mathbf{R}^+$ denote the multiplicative group of reals $> 0$. If $v$ is real, then $k_v^+ \cong \mathbf{R}^+$, and $k_v^*/k_v^+ \cong \{1, -1\}$. Consider the map

$$k^*(\mathfrak{c}) \to \prod_{\mathfrak{p}|\mathfrak{c}_0} (\mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}^{m(\mathfrak{p})}) \times \prod_{\substack{v|\mathfrak{c} \\ v \text{ real}}} k_v^*/k_v^+,$$

where as usual $m(\mathfrak{p})$ denotes the order of $\mathfrak{p}$ in $\mathfrak{c}$. Using the approximation theorem (theorem 2.22), we see that this map is surjective. By definition, its kernel is $k_{\mathfrak{c}}$.

**Definition 2.9** Let $\mathfrak{c}_0$ be a cycle containing finite primes only. For every $\mathfrak{p}|\mathfrak{c}$ let

$$\varphi_{\mathfrak{p}}(\mathfrak{c}_0) = \#(\mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}^{m(\mathfrak{p})})^*.$$

Define the **Euler $\varphi$-function** by

$$\varphi(\mathfrak{c}_0) = \prod_{\mathfrak{p}|\mathfrak{c}_0} \varphi_{\mathfrak{p}}(\mathfrak{c}_0).$$

Note that we have the tower of groups

$$k(\mathfrak{c}) \supset UK_{\mathfrak{c}} \supset k_{\mathfrak{c}},$$

hence

$$Uk_{\mathfrak{c}}/k_{\mathfrak{c}} \cong U/(U \cap k_{\mathfrak{c}}) = U/U_{\mathfrak{c}}.$$

Putting everything together gives the diagram

$$\begin{tikzcd}
& & I(\mathfrak{c}) \arrow[r, hook] \arrow[d, dash] & I \arrow[d, dash] \\
& k(\mathfrak{c}) \arrow[r, two heads] \arrow[d, dash] & P(\mathfrak{c}) \arrow[r, hook] \arrow[d, dash] & P . \\
U \arrow[r, hook] \arrow[d, dash] & Uk_{\mathfrak{c}} \arrow[r, two heads] \arrow[d, dash] & P_{\mathfrak{c}} & \\
U_{\mathfrak{c}} \arrow[r, hook] & k_{\mathfrak{c}} & &
\end{tikzcd}$$

Using this we can show, if we let $h_{\mathfrak{c}}$ denote the cardinality of $I(\mathfrak{c})/P_{\mathfrak{c}}$ and $h$ the class number of $k$ (i.e. the cardinality of the ordinary class group $I/P$):

**Theorem 2.10**

$$h_{\mathfrak{c}} = \frac{h\varphi(\mathfrak{c}_0)2^{s(\mathfrak{c})}}{(U : U_{\mathfrak{c}})}$$

*where $s(\mathfrak{c})$ is the number of real $v|\mathfrak{c}$.*

Proof By the diagram above,

$$\begin{aligned}
h_{\mathfrak{c}} &= \#I(\mathfrak{c})/P_{\mathfrak{c}} \\
&= \#I(\mathfrak{c})/P(\mathfrak{c}) \cdot \#P(\mathfrak{c})/P_{\mathfrak{c}} \\
&= \#(I/P) \cdot \#k(\mathfrak{c})/Uk_{\mathfrak{c}} \\
&= h \cdot \frac{\#k(\mathfrak{c})/k_{\mathfrak{c}}}{\#Uk_{\mathfrak{c}}/k_{\mathfrak{c}}} \\
&= \frac{h\varphi(\mathfrak{c}_0)2^{s(\mathfrak{c})}}{(U : U_{\mathfrak{c}})}.
\end{aligned}$$

■

**Corollary 2.11**

$$(U : U_{\mathfrak{c}}) < \infty.$$

Proof Otherwise we would have $h_{\mathfrak{c}} = 0$. ■

**Corollary 2.12** *Let $V$ be the group of units modulo roots of unity, and let $V_{\mathfrak{c}} = V \cap k_{\mathfrak{c}}$. Then $V$ and $V_{\mathfrak{c}}$ have the same rank as a $\mathbf{Z}$-module.*

Proof If the ranks were not equal, then $(V : V_{\mathfrak{c}})$ would not be finite, hence $(U : U_{\mathfrak{c}})$ would not be finite (the roots of unity have no influence on the finiteness). ■

**Corollary 2.13** *Let $\{\eta_1, \dots, \eta_r\}$ be independent roots generating $U_{\mathfrak{c}}$ modulo roots of unity (here $r = r_1 + r_2 - 1$, where $r_1$ is the number of real embeddings, $r_2$ the number of conjugate pairs of complex embeddings). Then the log-vectors $\{(\log |\sigma_j \eta_i|^{N_j})_j\}_i$ (with $N_j = 1$ if $\sigma_j$ is real and $N_j = 2$ if $\sigma_j$ is complex) generate a lattice in $\mathbf{R}^r$.*

Proof By the previous corollary, the log-vectors generate a subgroup of the lattice generated by $U$ (the last one is a lattice by the Unit Theorem, cf. Lang [9, section V.§1]) of the same rank as a **Z**-module. Hence this subgroup is also a lattice. ■

**Definition 2.14** We define the **$\mathfrak{c}$-regulator** $R_{\mathfrak{c}}$ by

$$R_{\mathfrak{c}} = |\det(\log |\sigma_j \eta_i|^{N_j})|.$$

**Corollary 2.15** *The regulator $R_{\mathfrak{c}}$ is non-zero.*

Proof Immediate by the previous corollary. ■

## 2.2 Ideals as lattices

We want to view fractional ideals as lattices in Euclidean space. For that we need a few prelimenaries, which will be developed next.

The following proposition is from Cohen [1, chapter 2, section 3].

**Proposition 2.16** *Let $L$ be a $\mathbf{Z}$-submodule of $\mathbf{R}^N$. Consider the following three conditions:*

*(1) $L$ generates $\mathbf{R}^N$ as an $\mathbf{R}$-vector space.*

*(2) $L$ is discrete.*

*(3) $L$ is a free $\mathbf{Z}$-module of rank $N$.*

*Then any two of these conditions implies the third.*

Proof Assume (1) and (2). Then (3) follows from proposition 1.3.

Assume (1) and (3). Let $b_1, \dots, b_N$ be a $\mathbf{Z}$-basis of $L$. Then $b_1, \dots, b_N$ is an $\mathbf{R}$-basis of $\mathbf{R}^N$. Consider the open neighborhoud $\Omega$ of 0 consisting of the $x = \sum_{i=1}^{n} x_i b_i$ with $|x_i| < 1$. Then the only element of $L$ in $\Omega$ is 0. Hence 0 is an isolated point of $L$, hence by translation of $\Omega$, every point of $L$ is. Hence $L$ is discrete.

Assume (2) and (3). Let $W$ be the $\mathbf{R}$-vector space generated by $L$. Then (1) and (2) hold with $V$ replaced by $W$. Hence by what we have proved, $L$ is a free $\mathbf{Z}$-module on $\dim(W)$ generators. Hence $\dim(W) = N$ by (3) and proposition 1.2. Hence $W = \mathbf{R}^N$. ■

The following propositions are from Sheppard and Osserman [13].

**Proposition 2.17** *Let $K$ be a number field, $\mathcal{O}_K$ its ring of integers, $\alpha \in K$. Then there is a non-zero $d \in \mathbf{Z}$ such that $d\alpha \in \mathcal{O}_K$.*

Proof There is an equation

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_0 = 0$$

with $a_i \in \mathbf{Z}$ and $a_n \neq 0$. Multiply it by $a_n^{n-1}$ to get:

$$(a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + \cdots + a_n^{n-1}a_0 = 0.$$

Hence $a_n\alpha$ is integral over $\mathbf{Z}$, hence $a_n\alpha \in \mathcal{O}_K$. ■

**Proposition 2.18** *Let $K$ be a number field, $\mathcal{O}_K$ the ring of integers. Then $K = \mathrm{Frac}(\mathcal{O}_K)$, the field of fractions of $\mathcal{O}_K$.*

Proof Note that $\mathcal{O}_K \subset K$, and since $\mathrm{Frac}(\mathcal{O}_K)$ is the smallest field containing $\mathcal{O}_K$, we have $\mathrm{Frac}(\mathcal{O}_K) \subset K$. Conversely, let $\alpha \in K$. Then by proposition 2.17 there is a non-zero $d \in \mathbf{Z}$ such that $d\alpha \in \mathcal{O}_K$. Thus $\alpha \in \mathrm{Frac}(\mathcal{O}_K)$. Hence $K = \mathrm{Frac}(\mathcal{O}_K)$. ■

**Proposition 2.19** *Let $K$ be a number field of degree $N$ over $\mathbf{Q}$. Then the ring of integers $\mathcal{O}_K$ is a $\mathbf{Z}$-module of rank $N$.*

Proof It is well known that the ring of integers of a number field is finitely generated as a $\mathbf{Z}$-module. (See for instance Lang [9, chapter 1, §2, proposition 6].) We get an inclusion

$$\mathbf{Q} \otimes_{\mathbf{Z}} \mathcal{O}_K \hookrightarrow K.$$

As rings however, $\mathbf{Q} \otimes_{\mathbf{Z}} \mathcal{O}_K = \mathbf{Q}[\mathcal{O}_K]$. The ring on the right is the smallest field containing $\mathcal{O}_K$. But this is equal to $K$. Hence $\mathbf{Q} \otimes_{\mathbf{Z}} \mathcal{O}_K = K$. Hence $\mathbf{Q} \otimes_{\mathbf{Z}} \mathcal{O}_K$ is a vector space of dimension $N$ over $\mathbf{Q}$, hence the rank of $\mathcal{O}_K$ as a $\mathbf{Z}$-module is $N$. ■

**Proposition 2.20** *Let $K$ be a number field of degree $N$ over $\mathbf{Q}$, $\mathfrak{a}$ an ideal of $K$. Then $\mathfrak{a}$ is a free $\mathbf{Z}$-module of rank $N$.*

Proof Let $d \in \mathcal{O}_K$ be non-zero such that $d\mathfrak{a} \subset \mathcal{O}_K$. Then $\mathfrak{a} \cong d\mathfrak{a}$ as $\mathbf{Z}$-modules, and as $\mathcal{O}_K$ is free of rank $N$, $\mathfrak{a}$ must be free of rank $\leq N$.

On the other hand, let $a \in \mathfrak{a} \setminus \{0\}$. Then $a\mathcal{O}_K \subset \mathfrak{a}$ and $a\mathcal{O}_K \cong \mathcal{O}_K$ as $\mathbf{Z}$-modules. Hence the rank of $\mathfrak{a}$ is also $\geq N$. ■

Let $K$ be a number field of degree $N$ over $\mathbf{Q}$. To apply our result of theorem 1.15 we need to be able to view an ideal $\mathfrak{a}$ of $K$ as a lattice in some Euclidean space. This Euclidean space will be the product of the completions of $K$ with respect to its Archimedean absolute values.

**Proposition 2.21** *Let $K$ be a number field, $|\cdot|_1, |\cdot|_2$ be two Archimedean absolute values, corresponding to embeddings $\sigma, \tau$ respectively. Then $|\cdot|_1$ and $|\cdot|_2$ are equivalent (induce the same topology on $K$) if and only if $\sigma$ and $\tau$ are conjugate embeddings: $\sigma \in \{\tau, \overline{\tau}\}$.*

Proof If $\sigma$ and $\tau$ are conjugate embeddings than clearly they induce the same topology on $K$.

Conversely, assume that $|\cdot|_1$ and $|\cdot|_2$ induce the same topology. Then one can show (see for instance Lang [9, page 32]) that one must be a power of the other: there is a $\lambda > 0$ such that $|\cdot|_1 = |\cdot|_2^\lambda$. Applying both norms to 2 shows that $2 = 2^\lambda$, hence that $\lambda = 1$. This shows that for every $x \in K$ we have $|\sigma(x)| = |\tau(x)|$. If $\sigma$ is real then for every $x$ we have that $\sigma(x)$ is uniquely determined by $|\sigma(x)|$ and $|\sigma(x) - 1|$. This then implies that $\tau$ is also real and equal to $\sigma$.

If both $\sigma$ and $\tau$ are complex, let $y \in K$ be such that $\sigma(y) \in \mathbf{C}$. There are precisely two points in $\mathbf{C}$ with distance $|\sigma(y)|$ to 0 and $|\sigma(y) - 1|$ to 1 and they are $\sigma(y)$ and $\overline{\sigma(y)}$. Either possibility determines $\tau$ completely, and we have that $\tau(y) = \sigma(y)$ implies $\tau = \sigma$, and $\tau(y) = \overline{\sigma(y)}$ implies $\tau = \overline{\sigma}$. ■

**Theorem 2.22 (Approximation Theorem)** *Let $K$ be a field, and $|\cdot|_1, \ldots, |\cdot|_s$ non-trivial pairwise independent absolute values on $K$. Let $x_1, \ldots, x_s$ be elements of $K$, and $\epsilon > 0$. Then there exists an $x \in K$ such that*

$$|x - x_i|_i < \epsilon$$

*for all $i$.*

Proof See Lang [9, theorem II.§1.1]. ■

**Definition 2.23** For a number field $K$, denote by $S_\infty$ the Archimedean absolute values.

From the general theory of separable extensions we know that $K$ has $N$ embeddings in $\mathbf{C}$. We know that the complex embeddings come in conjugate pairs. Hence, if we write $r_1$ for the number of real embeddings and $2r_2$ for the number of complex embeddings we have $r_1 + 2r_2 = N$.

**Proposition 2.24** *Let $K$ be a number field, $S_\infty$ its Archimedean absolute values, $r_1$ the number of real embeddings and $2r_2$ the number of complex embeddings. Then $\# S_\infty = r_1 + r_2$.*

Proof This is almost immediate by proposition 2.21. Two absolute values are equivalent if and only if they come from a pair of conjugate embeddings. ■

When $v$ is an Archimedean absolute value of $K$ we can form the completion of $K$ with respect to $v$. We denote this by $K_v$. If $v$ is real then $K_v = \mathbf{R}$, if $v$ is complex then $K_v = \mathbf{C}$. The Euclidean space we will embed our ideals in will be the following

$$A_K(\infty) = \prod_{v \in S_\infty} K_v = \mathbf{R}^N.$$

Let $\sigma_v$ denote an embedding in $\mathbf{C}$ for every Archimedean $v$ (fix one if $v$ is complex). We have the inclusion

$$\begin{aligned} K &\hookrightarrow \prod_{v \in S_\infty} K_v \\ x &\mapsto (\sigma_v(x))_v. \end{aligned}$$

We will show that under this inclusion, every fractional ideal $\mathfrak{a}$ of $K$ gets mapped to a lattice in $A_K(\infty)$. We will also consider the subset of $A_K(\infty)$ defined as

$$J_K(\infty) = \prod_{v \in S_\infty} K_v^*$$

**Proposition 2.25** *Let $K$ be a number field, $\mathfrak{a}$ a fractional ideal of $K$. Then the image of $\mathfrak{a}$ under the above inclusion is a lattice in $A_K(\infty)$.*

Proof Note that the inclusion is a morphism of $\mathbf{Z}$-modules. Hence the image of $\mathfrak{a}$ is a $\mathbf{Z}$-module of rank $N$ by proposition 2.20.

We have the following equality (see for instance Lang [9, chapter III, §3, prop 13])

$$\begin{aligned} D_{K/\mathbf{Q}}(\mathfrak{a}) &= (N_{\mathbf{Q}}^K(\mathfrak{a}))^2 D_{K/\mathbf{Q}}(\mathbf{Z}) \\ &= (N_{\mathbf{Q}}^K(\mathfrak{a}))^2 \Delta_K. \end{aligned}$$

The right hand side is a non-zero ideal. The left hand side is the ideal generated by all discriminants $D_{K/\mathbf{Q}}(W)$ where $W$ ranges over the bases of $K$ over $\mathbf{Q}$ with $W \subset \mathfrak{a}$. In particular, there exists such a basis $W = \{w_i\}_i$.

This implies that

$$D_{K/\mathbf{Q}}(W) = \mathrm{Det}(\sigma_i w_j)^2 \neq 0,$$

where $\sigma_i$ ranges over the embeddings of $K$ in $\mathbf{C}$. Hence $\{(\sigma_i w_j)_j\}_i$ is a basis of $\mathbf{C}^N$. We will show that this implies that $\{(\sigma_v(w_i))_v\}_i$ forms a basis of $\mathbf{R}^N$.

Let $\sigma_1, \ldots, \sigma_{r_1}$ be the real embeddings of $K$. Let $\tau_1, \ldots, \tau_{r_2}$ and their conjugates be the complex ones. Write $\tau_j w_\nu = x_{j\nu} + \sqrt{-1} y_{j\nu}$ with $x_{j\nu}, y_{j\nu} \in \mathbf{R}$. We need to show that the following determinant is non-zero:

$$\mathrm{Det}_1 = \begin{vmatrix} \sigma_1 w_1 & \cdots & \sigma_1 w_N \\ \vdots & & \vdots \\ \sigma_{r_1} w_1 & \cdots & \sigma_{r_1} w_N \\ x_{11} & \cdots & x_{1N} \\ y_{11} & \cdots & y_{1N} \\ \vdots & & \vdots \\ x_{N1} & \cdots & x_{NN} \\ x_{N1} & \cdots & x_{NN} \end{vmatrix}.$$

To do so, we use that $D_{L/\mathbf{Q}}(W) \neq 0$. This means written out that the following determinant is non-zero:

$$\mathrm{Det}_2 = \begin{vmatrix} \sigma_1 w_1 & \cdots & \sigma_1 w_N \\ \vdots & & \vdots \\ \sigma_{r_1} w_1 & \cdots & \sigma_{r_1} w_N \\ x_{11} + i y_{11} & \cdots & x_{1N} + i y_{1N} \\ \vdots & & \vdots \\ x_{N1} + i y_{N1} & \cdots & x_{NN} + i y_{NN} \\ x_{11} - i y_{11} & \cdots & x_{1N} - i y_{1N} \\ \vdots & & \vdots \\ x_{N1} - i y_{N1} & \cdots & x_{NN} - i y_{NN} \end{vmatrix}.$$

The determinant is of a matrix which first has $r_1$ rows corresponding to the real embeddings and then twice $r_2$ rows corresponding to the complex embeddings. After adding the last set of $r_2$ rows to the first, and then subtracting again, we see that up to sign $\mathrm{Det}_2 = 2^{r_2}\,\mathrm{Det}_1$. In particular, $\mathrm{Det}_1 \neq 0$.

Hence the image of the lattice $\mathfrak{a}$ is a $\mathbf{Z}$-module of rank $N$ and $\mathbf{R}$-linearly spans all of $\mathbf{R}^N$. This implies by proposition 2.16 that the image of $\mathfrak{a}$ under the inclusion is a lattice. ■

## 2.3 Asymptotic Behaviour of the Number of Integral Ideals of Bounded Norm going to Infinity

We will need the volume of a fundamental domain of $\mathfrak{a}$ viewed as a lattice in $\mathbf{R}^N$. We can continue where we left off in our previous proof to show the following.

**Proposition 2.26** *Let $\mathfrak{a}$ be an ideal of $K$, and let $F$ be a fundamental domain of $\mathfrak{a}$, as a lattice in $\mathbf{R}^N$. Then*

$$\mathrm{Vol}(F) = 2^{-r_2}\sqrt{|D_{K/\mathbf{Q}}(\mathfrak{a})|} = 2^{-r_2}\mathbf{N}\mathfrak{a}\sqrt{|\Delta_K|}$$

Proof Let $W$ be the basis of $\mathfrak{a}$ from the proof of proposition 2.25. We then have $D_{K/\mathbf{Q}}(\mathfrak{a}) = (\mathrm{Det}_1)^2 = (2^{r_2}\,\mathrm{Det}_2)^2$. But $\mathrm{Det}_2$ is the determinant for a set of basis vectors of the lattice $\mathfrak{a}$. Hence $\mathrm{Det}_2 = \mathrm{Vol}(F)$ and we obtain $\sqrt{|D_{K/\mathbf{Q}}(\mathfrak{a})|} = 2^{r_2}\,\mathrm{Vol}(F)$.

The second equality in the proposition is a direct consequence of the formula $D_{K/\mathbf{Q}}(\mathfrak{a}) = (N^K_{\mathbf{Q}}(\mathfrak{a}))^2\Delta_K$. (Note that $\mathbf{N}\mathfrak{a} = N^K_{\mathbf{Q}}\mathfrak{a}$ for every ideal $\mathfrak{a}$ of $K$.) ■

Let $K$ be a number field, $U \subset \mathcal{O}_K$ be the group of units. Then $U$ acts on $K$ by multiplication. But $U$ also acts on $A_K(\infty)$ as follows:

$$u \cdot (\xi_v)_v = (\sigma_v u \cdot \xi_v)_v$$

for all $u \in U, (\xi_v)_v \in A_K(\infty)$.

Let $\xi \in K$. We then have the following identity (see for instance Lang [9, chapter I, §7, proposition 22] ):

$$\mathbf{N}(\xi) = |N_{\mathbf{Q}}^K(\xi)|.$$

On the left hand side we have the norm of the principal ideal $(\xi)$. On the right hand side we have the norm of field extensions $\prod_\sigma \sigma(\xi)$ where $\sigma$ ranges over the elements of the Galois group. The right hand side satisfies (see for instance Lang [9, chapter II, §1, corollary 2]):

$$\begin{aligned} |N_{\mathbf{Q}}^K(\xi)| &= \left| \prod_{v \text{ Archimedean}} |\xi_v|_v \right| \\ &= \prod_{v \text{ Archimedean}} |\xi_v|_v \end{aligned}$$

where $\xi_v = \sigma_v \xi$ where $\sigma_v$ is a fixed embedding corresponding to $v$. This identity allows us to define the following function $\mathbf{N}$ which on $A_K(\infty)$ restricts to the usual norm on $K$:

$$\mathbf{N}((\xi_v)_v) = \prod_{v \text{ Archimedean}} |\xi_v|_v.$$

Note that for $u \in U$ we have $N_{\mathbf{Q}}^K(u) = \pm 1$ . Hence the function $\mathbf{N}$ is constant on orbits of $U$ and therefore factors through $A_K(\infty)/U$.

We will now extend the definition of $A_K(\infty)$ to be able to exclude primes.

**Definition 2.27** Let $K$ be a number field and $\mathfrak{c}$ a cycle. Then $A_K(\infty, \mathfrak{c})$ is the subset $A_K(\infty)$ consisting of those $(\xi_v)_v$ such that $\xi_v > 0$ if $v$ real, $v|\mathfrak{c}$. Likewise we define $J_K(\infty, \mathfrak{c})$ as the subset of $J_K(\infty)$ of thise $(\xi_v)_v$ such that $\xi_v > 0$ if $v$ real, $v|\mathfrak{c}$.

**Proposition 2.28** *Let $K$ be a number field, $U \subset \mathcal{O}_K$ the group of units, $U_\mathfrak{c} = U \cap K_\mathfrak{c}$ (as usual). Then $J_K(\infty, \mathfrak{c})$ is stable under the action of $U_\mathfrak{c}$.*

PROOF Let $u \in U_\mathfrak{c}$, $\xi = (\xi_v)_v \in J_K(\infty, \mathfrak{c})$. We will show that $u \cdot \xi \in J_K(\infty, \mathfrak{c})$. Clearly $\sigma_v u \neq 0$ for every $v$ real, $v|\mathfrak{c}$. Hence $\sigma_v u \cdot \xi_v \neq 0$ for all such $v$.

Furthermore $\sigma_v u > 0$ and $\xi_v > 0$ hence $\sigma_v u \xi_v > 0$. Hence indeed $u \cdot \xi \in J_K(\infty, \mathfrak{c})$. ■

**Definition 2.29** If a group $G$ acts on a set $X$ then a subset $D \subset X$ will be called a **fundamental domain** for the action if it contains a unique representative of every orbit of the action.

Let $V$ be the free part of the group $U_\mathfrak{c}$ (the torsion part being the roots of unity in $U_\mathfrak{c}$). Then the action of $U_\mathfrak{c}$ on $J_K(\infty, \mathfrak{c})$ restricts to an action of $V$ on $J_K(\infty, \mathfrak{c})$. For this action there is a fundamental domain with some nice properties.

**Proposition 2.30** *There exists a fundamental domain $D$ for the action of $V$ on $J_K(\infty, \mathfrak{c})$ such that $tD = D$ for all $t > 0$ and such that $D(1)$ (the subset of $D$ of those $\xi$ such that $\mathbf{N}\xi \leq 1$) has a $(N-1)$-Lipschitz parametrizable boundary.*

Proof We will postpone the proof. The proof of this proposition will be given in the proof of theorem 2.33. First we will show some of the implications. ■

Let $\mathcal{R}$ be a class of $I(\mathfrak{c})/P_{\mathfrak{c}}$. Let $t > 0$ We wish to count the number of integral ideals $\mathfrak{a} \in \mathcal{R}$ such that $\mathbf{N}\mathfrak{a} \leq t$. Denote this number by $j(\mathcal{R}, t)$.

Let $\mathfrak{b} \in \mathcal{R}^{-1}$. Then $\mathfrak{b}$ has a factorization:

$$\mathfrak{b} = \frac{\mathfrak{p}_1 \cdots \mathfrak{p}_s}{\mathfrak{q}_1 \cdots \mathfrak{q}_r},$$

and all ideals in this factorization are prime to $\mathfrak{c}$. The $\mathfrak{c}$-class group is finite, say of order $h_{\mathfrak{c}}$. Then $(\mathfrak{q}_1 \cdots \mathfrak{q}_r)^{h_{\mathfrak{c}}} = (\alpha)$ for some $\alpha \in K_{\mathfrak{c}}$. Hence

$$(\alpha)\mathfrak{b} = \mathfrak{p}_1 \cdots \mathfrak{p}_s (\mathfrak{q}_1 \cdots \mathfrak{q}_r)^{h_{\mathfrak{c}}-1}.$$

Hence we have found an element of $\mathcal{R}^{-1}$ that is an integral ideal. Hence we can assume without loss of generality that $\mathfrak{b}$ is integral.

Consider the map

$$\mathfrak{a} \mapsto \mathfrak{a}\mathfrak{b} = (\xi) \mapsto \xi \pmod{U_{\mathfrak{c}}} \in K_{\mathfrak{c}}/U_{\mathfrak{c}}$$

from integral ideals of $I(\mathfrak{c})$ to $U_{\mathfrak{c}}$-equivalence classes of elements $\xi$ satisfying

$$\begin{aligned} \xi &\equiv 1 \quad (\text{mod}^* \mathfrak{c}), \\ \xi &\equiv 0 \quad (\text{mod } \mathfrak{b}). \end{aligned}$$

This is well defined because certainly these $\xi \in K_{\mathfrak{c}}$ (i.e. $\xi \equiv 1 \ (\text{mod}^* \mathfrak{c})$). Furthermore if $(\xi) = (\xi')$ then there is a $u \in U$ such that $\xi = u\xi'$. But this shows that $u = \xi/\xi'$, hence that $u \in K_{\mathfrak{c}}$, hence that $u \in U_{\mathfrak{c}}$. And lastly $\mathfrak{a}$ and $\mathfrak{b}$ are integral ideals hence $\mathfrak{a}\mathfrak{b} = (\xi)$ implies $\xi \equiv 0 \pmod{\mathfrak{b}}$.

We will show that this map is in fact a bijection.

Suppose $\mathfrak{a}$ and $\mathfrak{b}$ get mapped to the same element of $K_{\mathfrak{c}}/U_{\mathfrak{c}}$. That implies that $\mathfrak{a}\mathfrak{b} = \mathfrak{a}'\mathfrak{b}$. Multiplying by $\mathfrak{b}^{-1}$ shows that $\mathfrak{a} = \mathfrak{a}'$. Hence the map is injective.

Lastly let $\xi \equiv 1 \ (\text{mod}^* \mathfrak{c})$, $\xi \equiv 0 \pmod{\mathfrak{b}}$ represent an $U_{\mathfrak{c}}$-equivalence class. Then $(\xi)$ is an integral ideal in $P_{\mathfrak{c}}$. Hence $\mathfrak{a}(\xi) \in \mathcal{R}$, and this gets mapped to $\mathfrak{b}\mathfrak{a}(\xi) = (\xi)$. Hence the map is surjective. Note that $\mathbf{N}\mathfrak{a} \leq t$ if and only if $\mathbf{N}\mathfrak{a}\mathfrak{b} = \mathbf{N}(\xi) \leq \mathbf{N}\mathfrak{b} \cdot t$.

**Proposition 2.31** *Let $K$ be a number field, $U_{\mathfrak{c}}$ the group of $\mathfrak{c}$-units, $V$ the free subgroup. Let $D$ be a fundamental domain for the action of $V$ on $J_K(\infty, \mathfrak{c})$. Let $w_{\mathfrak{c}}$ be the the number of roots of unity in $K_{\mathfrak{c}}$, that is the cardinality of the torsion part of $U_{\mathfrak{c}}$.*

*Then every $U_{\mathfrak{c}}$-class has exactly $w_{\mathfrak{c}}$ representatives in $D$.*

Proof Note that $U_\mathfrak{c}$ acts transitively on $J_K(\infty,\mathfrak{c})$. Write $U_\mathfrak{c} = \mu_\mathfrak{c} \times V_\mathfrak{c}$ where $\mu_\mathfrak{c}$ are the roots of unity in $U_\mathfrak{c}$ and $V_\mathfrak{c}$ is the free part. Let $C$ be a $U_\mathfrak{c}$-class. Let $\xi \in C$.

$$\begin{aligned} C &= \bigcup_{r\in\mu}\bigcup_{v\in V}\{rv\xi\} \\ &= \bigcup_{r\in\mu}\underbrace{\left(\bigcup_{v\in V}\{v(r\xi)\}\right)}_{V\text{-class}} \end{aligned}$$

Hence $C$ is the disjoint union of $V$-classes, one for every $r \in \mu$. Every one contains precisely one element of $D$, hence we get $w_\mathfrak{c}$ representatives in $D$ in total. ■

Hence we see that if we count the number of elements of $D$ satisfying section 2.3 and $\mathbf{N}(\xi) \leq t$ we get $w_\mathfrak{c} j(\mathcal{R},t)$. That is, $w_\mathfrak{c} j(\mathcal{R},t)$ is equal to the number of elements $\xi$ satisfying

$$\begin{cases} \xi \in \mathfrak{b}, \\ \xi \equiv 1 \pmod{\mathfrak{c}_0}, \\ \xi \in D(\mathbf{N}\mathfrak{b}\cdot t) = (\mathbf{N}\mathfrak{b}\cdot t)^{1/N}D(1). \end{cases}$$

We actually need $\xi \equiv 1 \ (\text{mod}^*\mathfrak{c})$, but $\xi \equiv 1 \pmod{\mathfrak{c}_0}$ is enough, since the third condition implies $\xi \in D$, hence $\xi \in J_k(\infty,\mathfrak{c})$, hence $\sigma_v\xi > 0$ if $v$ is real, $v|\mathfrak{c}$.

The two congruences

$$\xi \equiv 0 \pmod{\mathfrak{b}} \text{ and } \xi \equiv 1 \pmod{\mathfrak{c}_0}$$

define a translation of the lattice given by the ideal $\mathfrak{b}\mathfrak{c}_0$ in $R^N = A_k(\mathfrak{c})$, by the Chinese Remainder Theorem. To be precise, if $\xi_0$ is a solution to the system above, then

$$\xi \mapsto \xi - \xi_0$$

gives a bijection between these congruences and $\mathfrak{b}\mathfrak{c}_0$ (note that the Chinese Remainder Theorem applies since $\mathfrak{b}$ and $\mathfrak{c}_0$ are relatively prime). Thus we see:

**Lemma 2.32** *Let $L$ be the lattice obtained by translating the lattice of $\mathfrak{b}\mathfrak{c}_0$ by the solution $\xi_0$. Then $w_\mathfrak{c} j(\mathcal{R},t)$ is equal to the number of elements in*

$$(\mathbf{N}\mathfrak{b}\cdot t)^{1/N}D(1).$$

Hence we can apply theorem 1.18. Hence we have, save for the construction of the fundamental domain $D$ of the action of $V$ on $J_k(\infty,\mathfrak{c})$ and the computation of its volume,

**Theorem 2.33** *Let $\mathfrak{c}$ be a cycle of $k$, $R$ a class of $I(\mathfrak{c})$ modulo $P_\mathfrak{c}$. Then*

$$j(\mathcal{R},t) = \rho_c t + O(t^{1-1/N}),$$

*where*

$$\rho_c = \frac{2^{r_1}(2\pi)^{r_2} R_{\mathfrak{c}}}{w_{\mathfrak{c}}\sqrt{|\Delta_k|}\mathbf{N}\mathfrak{c}}$$

*and:*

- $R_{\mathfrak{c}}$ *is the* $\mathfrak{c}$*-regulator,*
- $\mathbf{N}\mathfrak{c} = 2^{s(\mathfrak{c})}\mathbf{N}\mathfrak{c}_0$*,*
- $s(\mathfrak{c})$ *is the number of real* $v|\mathfrak{c}$*,*
- $w_{\mathfrak{c}}$ *is the number of roots of unity in* $U_{\mathfrak{c}}$*,*
- $\Delta_k$ *is the discriminant of* $k$*.*

Proof By lemma lemma 2.32, the only thing that remains is to construct a fundamental domain $D$ of the action of $V$ on $J_k(\infty, \mathfrak{c})$, such that $tD = D$, $\partial D$ is $(N-1)$-Lipschitz parametrizable, and

$$\operatorname{Vol} D(1) = 2^{r_1 - s(\mathfrak{c})}\pi^{r_2} R_{\mathfrak{c}}.$$

First we shall construct $D$. Let $g$ be the map

$$\begin{aligned} g\colon J_k(\infty,\mathfrak{c}) &\to \prod_{v\in S_\infty} \mathbf{R}_v, \\ (\xi_v)_v &\mapsto \left(\log \frac{\|\xi_v\|}{\mathbf{N}\xi^{N_v/N}}\right)_v. \end{aligned}$$

Then the image of $g$ is contained in the hyperplane of those $z$ such that

$$\sum_{v\in S_\infty} z_v = z_1 + \cdots z_{r_1+r_2} = 0.$$

Let $\{\eta_1, \ldots, \eta_r\}$ be generators for $V$, the group generated by $U_{\mathfrak{c}}$ without the roots of unity. Set $y_i = g(\eta_i)$. Then by the corollary 2.13, $\{y_1, \ldots, y_r\}$ is a basis for a lattice $H$ (note that $\mathbf{N}\eta_i = 1$). Let $F$ be the fundamental domain of $H$ given by the linear combinations

$$c_1 y_1 + \cdots + c_r y_r \qquad 0 \le c_q < 1.$$

Set $D = g^{-1}(F)$. Then $D$ is a fundamental domain for the action of $V$ on $J_k(\infty, \mathfrak{c})$, for for $(\xi_v)_v \in J_k(\infty, \mathfrak{c})$,

$$g((\eta_1^{k_1}\cdots\eta_r^{k_r})(\xi_v)_v) = g(\xi) + k_1 y_1 + \cdots k_r y_r.$$

Let $t > 0$. Then

$$\left(\frac{\|t\xi_v\|}{\mathbf{N}(t\xi)^{N_v/N}}\right)_v = \left(\frac{\|\xi_v\|}{\mathbf{N}\xi}\right)_v,$$

hence $(\xi_v)_v \in D$ if and only if $g((\xi_v)_v) \in F$ if and only if $g((t\xi_v)_v) \in F$ if and only if $t(\xi_v)_v \in D$. Hence $tD = D$.

For $\xi \in D$ we have

$$\log \frac{\|\xi_v\|^{N_v}}{\mathbf{N}\xi^{N_v/N}} \leq Br$$

where $B$ is the maximum of the $|y_q|$. Hence we get

$$|\xi_v| \leq \max(1, |\xi_v|^{N_v}) \leq \max(1, \mathbf{N}\xi^{1/N} e^{Br})$$

Hence $D(1)$ is bounded, and for $\xi \in D(1)$ we get, if we let $B > 1$:

$$|\xi_v| \leq e^{Br}.$$

What is left to do is to show that $\partial(D(1))$ is $(N-1)$-Lipschitz parametrizable, and to compute $\operatorname{Vol} D(1)$. We use polar coordinates $(\rho, \vartheta_i)$ $(i = 1, \dots, r_1 + r_2)$ to do this. We let $0 \leq \rho_i$ for all $i$ and $\vartheta_i = \pm 1$ if $i = 1, \dots, r_1$, but $\vartheta_i = 1$ if $v_i | \mathfrak{c}$. If $i = r_1 + 1, \dots, r_1 + r_2$ we let $0 \leq \vartheta_i \leq 2\pi$. Map $((\rho_i, \vartheta_i))_i$ to $(\rho_i e^{i\vartheta_i})_i$. The inverse image of $D(1)$ in polar coordinate space is given by those $(\xi_{v_j})_j = (\xi_j)_j = (\rho_j e^{i\vartheta_j})_j$ such that

$$\left\{ \begin{array}{l} 0 < \prod_{i=1}^{r_1+r_2} \rho_i^{N_i} \leq 1, \\ \log \rho_j - \frac{1}{N} \log \prod_{i=1}^{r_1+r_2} \rho_i^{N_i} = \sum_{q=1}^{r} c_q \log |\sigma_j \eta_q| \quad j = 1, \dots, r_1 + r_2. \end{array} \right. \tag{2.2}$$

The first condition is equivalent to $\mathbf{N}\xi \leq 1$, the second condition (or actually, the next $r_1 + r_2$ conditions) is (are) equivalent to $\xi \in D$. Hence both conditions together are equivalent to $\xi \in D(1)$. Note that none of the equations from eq. (2.2) involve any of the angles $\vartheta_i$. Let $P$ denote the set of $(\rho_1, \dots, \rho_{r_1+r_2})$ that satisfy eq. (2.2). then

$$\begin{aligned} \operatorname{Vol} D(1) &= \int_{D(1)} 1 \, d\xi_1 \cdots d\xi_{r_1+r_2} \\ &= \underset{P}{\int \cdots \int} \int_0^{2\pi} \cdots \int_0^{2\pi} \int_{\{\pm 1\}} \cdots \int_{\{\pm 1\}} \int_{\{1\}} \cdots \int_{\{1\}} \rho_{r_1+1} \cdots \rho_{r_1+r_2} \\ &\quad d\vartheta_1 \cdots d\vartheta_{s(\mathfrak{c})} \, d\vartheta_{s(\mathfrak{c})+1} \cdots d\vartheta_{r_1} \, d\vartheta_{r_1+1} \cdots d\vartheta_{r_1+r_2} \, d\rho_1 \cdots d\rho_{r_1+r_2} \\ &= 2^{r_1 - s(\mathfrak{c})} (2\pi)^{r_2} \underset{P}{\int \cdots \int} \rho_{r_1} \cdots \rho_{r_1+r_2} \, d\rho_1 \cdots d\rho_{r_1+_2}. \end{aligned}$$

We change variables again. Consider the cube $S$ in $(r_1 + r_2)$-space with variables $(u, c_1, \dots, c_r)$ such that

$$\left\{ \begin{array}{ll} 0 < u \leq 1, & \\ 0 \leq c_q < 1 & \quad (q = 1, \dots, r) \end{array} \right.$$

We have a bijection $f \colon S \to P$ between this cube $S$ and $P$, given in one direction by

$$\rho_j = u^{1/N} \exp\left( \sum_{q=1}^{r} c_q \log |\sigma_j \eta_q| \right).$$

That the image of $f$ is indeed contained in $P$ follows from first considering the product

$$\begin{aligned}\prod_{j=1}^{r_1+r_2} \rho_j^{N_j} &= u \exp\left(\sum_{q=1}^{r} c_q \log\left(\prod_{j=1}^{r_1+r_2} |\sigma_j \eta_q|^{N_j}\right)\right)\\ &= u \exp\left(\sum_{q=1}^{r} c_q \log |N_{\mathbf{Q}}^{k}(\eta_q)|\right)\\ &= u,\end{aligned}$$

since $N_{\mathbf{Q}}^{k}(\eta_q) = \pm 1$, since $\eta_q$ is a unit. Since $0 < u \leq 1$, the first condition of 2.2 is satisfied. As a direct consequence, the second condition is also satisfied. (Apply log to the expression of $\rho_j$ and use the identity above for $u$.) Hence the image of $f$ is indeed contained in $P$.

To show that it is a bijection, we show the existence of an inverse. We already saw that

$$\prod_{j=1}^{r_1+r_2} \rho_j^{N_j} = u.$$

The numbers $c_q$ are uniquely determined by $(\rho_1, \ldots, \rho_{r_1+r_2})$ because

$$\det(\log |\sigma_j \eta_q|^{N_j})_{jq} = R_{\mathfrak{c}}$$

does not vannish (corollary 2.15)

We compute the Jacobian determinant. First compute the partial derivatives:

$$\frac{\partial \rho_j}{\partial u} = \frac{1}{N}\frac{\rho_j}{u} \text{ and } \frac{\partial \rho_j}{\partial c_q} = \rho_j \log |\sigma_j \eta_q|.$$

Hence the Jacobian determinant of $f$ is

$$\begin{aligned}&\begin{vmatrix} \frac{1}{N}\frac{\rho_1}{u} & \rho_1 \log |\sigma_1 \eta_1| & \cdots & \rho_1 \log |\sigma_1 \eta_{r_1+r_2}| \\ \vdots & \vdots & & \vdots \\ \frac{1}{N}\frac{\rho_{r_1+r_2}}{u} & \rho_{r_1+r_2} \log |\sigma_{r_1+r_2} \eta_1| & \cdots & \rho_{r_1+r_2} \log |\sigma_{r_1+r_2} \eta_{r_1+r_2}| \end{vmatrix}\\ &\quad = \frac{\prod_{j=1}^{r_1+r_2} \rho_j}{uN} \begin{vmatrix} 1 & \log |\sigma_1 \eta_1| & \cdots & \log |\sigma_1 \eta_{r_1+r_2}| \\ \vdots & \vdots & & \vdots \\ 1 & \log |\sigma_{r_1+r_2} \eta_1| & \cdots & \log |\sigma_{r_1+r_2} \eta_{r_1+r_2}| \end{vmatrix}.\end{aligned}$$

Adding the first $r = r_1 + r_2 - 1$ rows to the last after multiplying the $j$-th row by $N_j$ shows that this is equal to

$$\frac{1}{N\rho_{r_1+1}\cdots\rho_{r_1+r_2}}2^{-r_2}\begin{vmatrix} 1 & \log|\sigma_1\eta_1| & \cdots & \log|\sigma_1\eta_r| \\ \vdots & \vdots & & \vdots \\ 1 & \log|\sigma_r\eta_r| & \cdots & \log|\sigma_r\eta_r| \\ N & 0 & \cdots & 0 \end{vmatrix}$$
$$= \frac{1}{N\rho_{r_1+1}\cdots\rho_{r_1+r_2}}2^{-r_2}R_{\mathfrak{c}}.$$

Hence:

$$\begin{aligned}\operatorname{Vol} D(1) &= 2^{r_1-s(\mathfrak{c})}(2\pi)^{r_2}\int_S 2^{-r_2}R_{\mathfrak{c}}\,d\mu \\ &= 2^{r_1-s(\mathfrak{c})}\pi^{r_2}R_{\mathfrak{c}}\end{aligned}$$

where $\mu$ is the Lebesgue measure.

As to Lipschitz parametrizability, a continuously differentiable map from the cube $S$ to $P$ would suffice, since the closed cube $S$ is Lipschitz parametrizable. The only non-continuously differentiable aspect we encountered along the way of our reparametrizations was the exponent $1/N$ of $u$. But we can remedy this by doing one more reparametrization: reparametrize the unit cube $S$ by a copy of itself $S'$ with variables $(u', c'_1, \ldots, c'_r)$ and mapping this to $(u'^N, c'_1, \ldots, c'_r)$.■

# Chapter 3

# Representation theory of finite groups

We will use some representation theory of finite groups, which will be developed here. $G$ will always be a finite group. Our vector spaces will be over $\mathbf{C}$ and finite dimensional. The references for this section are Serre [11] and Lang [8].

**Definition 3.1** Let $G$ be a finite group and $V$ a $\mathbf{C}$-vector space. A **representation** of $G$ in $V$ is a homomorphism

$$G \to \operatorname{Aut}(V).$$

We call $\dim V$ the **degree** of the representation.

**Example 3.2** Let $G$ be a group. Let $R$ be the free $\mathbf{C}$-vector space generated by basis elements $e_\sigma$ with $\sigma \in G$. Define the **regular representation** of $G$ by $\rho_\sigma(e_\tau) = e_{\sigma\tau}$ for all $\sigma, \tau \in G$.

**Definition 3.3** Let $\rho\colon G \to \operatorname{Aut}(V)$ be a representation. We also denote $\rho(g)v$ by $gv$. The map $\rho(g)$ will also be denoted by $\rho_g$. We define $\mathbf{C}[G]$ to be the set of expressions of the form

$$\sum_{\sigma \in G} a_\sigma \sigma.$$

with $a_\sigma \in \mathbf{C}$ and all but finitely many $a_\sigma = 0$. With the natural addition and multiplication and multiplication with $\mathbf{C}$ this is a $\mathbf{C}$-algebra.

**Proposition 3.4** *There is a 1-1 correspondence between* $\mathbf{C}$*-algebra homomorphisms*

$$\mathbf{C}[G] \to \operatorname{End}(V)$$

*and representations*

$$G \to \operatorname{Aut}_{\mathbf{C}}(V).$$

Proof Restricting a $\mathbf{C}$-algebra homomorphism $\mathbf{C}[G] \to \mathrm{End}(V)$ to $G$ gives a representation and extending a representation $G \to \mathrm{Aut}(V)$ gives a $\mathbf{C}$-algebra homomorphism, and these operations are inverse to each other. ■

We will also call $\mathbf{C}$-algebra homomorphisms $\mathbf{C}[G] \to \mathrm{End}(V)$ representations of $G$. This is justified by proposition 3.4.

**Notation 3.5** We will sometimes abuse notation and for a representation

$$\rho \colon G \to \mathrm{Aut}(V)$$

write $\rho$ for the vector space $V$ and $V$ for the map $\rho$. This will cause no confusion.

**Theorem 3.6 (Maschke's Theorem)** *Let $\rho \colon G \to \mathrm{Aut}(V)$ be a representation. Let $W \subset V$ be a $G$-stable linear subspace. Then there exists a complement $W^0$ of $W$ (i.e. $W \oplus W^0 = V$) which is also $G$-stable.*

Proof Let $W'$ be an arbitrary complement of $W$ in $V$. Let $\pi \colon W \oplus W' = V \to W$ be the projection. Define $\pi^0$ by averaging this projection:

$$\pi^0 = \frac{1}{\#G} \sum_{\sigma \in G} \rho_\sigma \pi \rho_\sigma^{-1}.$$

Since $\pi$ maps $V$ into $W$, and $\pi_0$ preserves $W$, we see that $\pi_0$ maps $V$ into $W_0$.

We have $\pi_\sigma^{-1} x \in W$ for $x \in W$, hence

$$\begin{aligned} \pi\rho_\sigma^{-1} x &= \rho_\sigma^{-1} x, \text{ hence} \\ \rho_\sigma \pi \rho_\sigma^{-1} x &= x, \end{aligned}$$

hence $\pi^0 x = x$. Hence $\pi^0$ is a projection of $V$ onto $W$, corresponding to some complement $W^0$ of $W$. One readily verifies that $\rho_\sigma \pi^0 = \pi^0 \rho_\sigma$ for all $\sigma \in G$. If $x \in W^0$ and $\sigma \in G$ then $\pi^0 x = 0$, hence $\pi^0 \rho_\sigma x = \rho_\sigma \pi^0 x = 0$, i.e. $\rho_\sigma x \in W^0$, i.e. $W^0$ is stable under $G$. ■

**Definition 3.7** Suppose $\rho \colon G \to \mathrm{Aut}(V)$ is a representation. Suppose $W \subset V$ is a $G$-stable subspace. We then have a representation $\rho^W : G \to \mathrm{Aut}(W)$ by restricting each $\rho(\sigma)$ to $W$. The representation $\rho^W$ is called a **subrepresentation** of $\rho$.

**Definition 3.8** A representation $\rho \colon G \to \mathrm{Aut}(V)$ is said to be **simple** or **irreducible** if $V$ ahas no invariant subspaces other than 0 and $V$ itself. By theorem 3.6 this is equivalent to saying that $\rho$ is not the direct sum of two representations.

**Theorem 3.9** *Every representation is a direct sum of irreducible representations.*

Proof Induction on $\dim V$. If $\dim V = 0$ then $\rho$ is the empty direct sum of irreducible representations. Suppose $\dim V \geq 1$. If $\rho$ is irreducible, then we are done. Otherwise, $V$ can be decomposed by theorem 3.6 as $V \oplus V'$, both $G$-stable and of dimension smaller than $\dim V$. By induction both summands are the direct sum of irreducible representation, hence the total direct sum is. ■

**Definition 3.10** Two representations $\rho \colon G \to \mathrm{Aut}(V)$ and $\rho' \colon G \to \mathrm{Aut}(V')$ are called **isomorphic** if there is a linear isomorphism $\tau \colon V \to V'$ such that for all $\sigma \in G$:

$$\begin{tikzcd}
V \arrow[r, "\tau"] \arrow[d, "\rho(s)"] & V' \arrow[d, "\rho'(s)"] \\
V \arrow[r, "\tau"] & V'
\end{tikzcd}$$

commutes.

**Definition 3.11** Let $\rho^1 \colon G \to \mathrm{Aut}(V^1)$ and $\rho^2 \colon G \to \mathrm{Aut}(V^2)$ be two representations. We then define the following.

(1) The **direct sum representation** $\rho^1 \oplus \rho^2 \colon G \to \mathrm{Aut}(V^1 \oplus V^2)$ by

$$(\rho^1 \oplus \rho^2)_\sigma = \rho^1_\sigma \oplus \rho^2_\sigma$$

for all $\sigma \in G$.

(2) The **tensor product representation** $\rho^1 \otimes \rho^2 \colon G \to \mathrm{Aut}(V^1 \otimes V^2)$ by

$$(\rho^1 \otimes \rho^2)_\sigma = \rho^1_\sigma \otimes \rho^2_\sigma$$

for all $\sigma \in G$.

**Proposition 3.12 (Schur's Lemma)** *Let $\rho^1 \colon G \to \mathrm{Aut}(V^1)$ and $\rho^2 \colon G \to \mathrm{Aut}(V^2)$ be two irreducible representations of $G$. Let $f \colon V^1 \to V^2$ be a linear map such that*

$$\begin{tikzcd}
V \arrow[r, "f"] \arrow[d, "\rho^1(s)"] & V' \arrow[d, "\rho^2(s)"] \\
V \arrow[r, "f"] & V'
\end{tikzcd}$$

*commutes. Then*

*(1) If $\rho^1$ and $\rho^2$ are not isomorphic, then $f = 0$.*

*(2) If $V^1 = V^2$ and $\rho^1 = \rho^2$, $f$ is a homothety (i.e. a scalar multiple of the identity).*

Proof (1) The case $f = 0$ is trivial. Suppose $f \neq 0$. For $x \in \ker f$, we have $f\rho^1_s x = \rho^2_s f x = 0$, hence $\rho^1_s x \in \ker f$. Hence $\ker f$ is $G$-stable. Since $V_1$ is irreducible, this implies $\ker f = 0$ or $V^1$, but the second case is excluded by $f \neq 0$.

A similar argument shows that $\mathrm{Im}\, f = V^2$.

Hence $f$ is an isomorphism.

(2) Suppose $V^1 = V^2$, $\rho^1 = \rho^2$. Let $\lambda$ be an eigenvalue of $f$ (this exists because we work over **C**.) Put $f' = f - \lambda$. Since $\lambda$ is an eigenvalue of $f$, $\ker f' \neq 0$. On the other hand, by linearity of the $\rho_\sigma$, we have $\rho^2_\sigma \circ f' = f' \circ \rho^1_s$. By part (1) this implies that $f' = 0$, that is, $f = \lambda$. ■

**Corollary 3.13** *Let $h\colon V^1 \to V^2$ be linear. Put*

$$h^0 = \frac{1}{\#G} \sum_{\sigma \in G} (\rho^2_\sigma)^{-1} h \rho^1_\sigma.$$

*Then:*

*(1) If $\rho^1$ and $\rho^2$ are not isomorphic, $h^0 = 0$.*

*(2) If $V^1 = V^2 = V$, $\rho^1 = \rho^2 = \rho$, then $h^0$ is a homothety of ratio $\frac{1}{n}\operatorname{Tr} h$, with $n = \dim V$.*

Proof We have $\rho^2_\sigma h^0 = h^0 \rho^1_\sigma$, because

$$\begin{aligned}(\rho^2_\sigma)^{-1} h^0 \rho^1_\sigma &= \frac{1}{\#G} \sum_{\tau \in G} (\rho^2_\sigma)^{-1} (\rho^2_\tau) h \rho^1_\tau \rho^1_\sigma \\ &= \frac{1}{\#G} \sum_{\tau \in G} (\rho^2_{\tau\sigma})^{-1} h \rho^1_{\tau\sigma} \\ &= h^0.\end{aligned}$$

Apply Schur's lemma to $f = h^0$. We see in case (1) that $h^0 = 0$, and in case (2) that $h^0$ is equal to some scalar $\lambda$. In the second case we have

$$\begin{aligned}\operatorname{Tr} h_0 &= \frac{1}{\#G} \sum_{\tau \in G} \operatorname{Tr}((\rho_\tau)^{-1} h \rho_\tau) \\ &= \operatorname{Tr} h\end{aligned}$$

and since $\operatorname{Tr}\lambda = n\lambda$, we get $\lambda = \frac{1}{n}\operatorname{Tr} h$. ■

**Remark 3.14** Computations with matrix coefficients can lead to enormous amounts of indices. We give a short description of what happens when one computes with matrix coefficients so that in what follows the focus can be on the conceptual things. We write the coefficients of a matrix $A$ as $A_{ji}$, where the $j$ indicates the row and the $i$ the column. If $B_{kj}$ is then another matrix we have

$$(BA)_{ki} = \sum_j B_{kj} A_{ji}$$

If $C_{lk}$ is another matrix still we have

$$(CBA)_{li} = \sum_{k,j} C_{lk} B_{kj} A_{ji}.$$

This should make the pattern clear.

Fix bases of $V^1$ and $V^2$ and write all matrices with respect to these bases. Then

$$\begin{aligned}\rho^1_\tau &= (r_{i_1j_1}(\tau)),\\ \rho^2_\tau &= (r_{i_2j_2}(\tau)),\\ h &= (x_{i_2i_1}),\\ h^0 &= (x^0_{i_2i_1}).\end{aligned}$$

By definition of $h^0$ we have

$$x^0_{i_2i_1} = \frac{1}{\#G}\sum_{\tau,j_2,j_2} r_{i_2j_2}(\tau^{-1})x_{j_2j_1}r_{j_1i_1}(\tau).$$

The right hand side is a linear form with respect to $x_{j_2j_1}$. In case (1), this form is trivial, whence all its coefficients are zero. Therefore:

**Corollary 3.15** *In case (1) we have*

$$\frac{1}{\#G}\sum_{\tau\in G} r_{i_1j_2}(\tau^{-1})r_{j_1i_1}(\tau) = 0$$

*for arbitrary* $i_1, i_2, j_1, j_2$.

In case (2) we have $h^0 = \lambda$, i.e. $x^0_{i_2i_1} = \lambda\delta_{i_2i_1}$ (where $\delta$ is the Kronecker delta symbol), with $\lambda = \frac{1}{n}\operatorname{Tr}(h)$. That is

$$\lambda = \frac{1}{n}\sum_{j_2,j_1}\delta_{j_2j_1}x_{j_2j_1}.$$

Hence

$$\frac{1}{\#G}\sum_{\tau,j_1,j_2} r_{i_2j_2}(\tau^{-1})x_{j_2j_1}r_{j_1i_1}(\tau) = \frac{1}{n}\sum_{j_1,j_2}\delta_{i_1i_2}\delta_{j_2j_1}x_{j_2j_1}.$$

Equating coefficients of $x_{j_2j_1}$ we obtain:

**Corollary 3.16** *In case (2) we have*

$$\begin{aligned}\frac{1}{\#G}\sum_{\tau\in G} r_{i_2j_2}(\tau^{-1})r_{j_1i_1}(\tau) &= \frac{1}{n}\delta_{i_2i_1}\delta_{j_2j_1}\\ &= \begin{cases}\frac{1}{n} & \textit{if } i_1 = i_2 \textit{ and } j_1 = j_2,\\ 0 & \textit{otherwise.}\end{cases}\end{aligned}$$

**Definition 3.17** Let $\rho\colon G \to \operatorname{Aut}(V)$ be a representation. Pick a basis of $V$ and write $\rho_\sigma$ as a matrix with respect to this basis. Define the **character** $\chi_\rho$ of the representation $\rho$ as the map

$$\chi_\rho(\sigma) = \operatorname{Tr}(\rho_\sigma)$$

This is independent of choice of basis of $V$. It is the sum of eigenvalues of $\rho_\sigma$, counted with multiplicities.

**Proposition 3.18** *If $\chi_\rho$ is the character of a representation $\rho$ of degree $n$ then*

*(1)* $\chi(1) = n$,

*(2)* $\chi(\sigma^{-1}) = \overline{\chi(\sigma)}$ *for all* $\sigma \in G$,

*(3)* $\chi(\tau\sigma\tau^{-1}) = \chi(\sigma)$ *for* $\sigma, \tau \in G$.

Proof (1) The sum of the diagonal elements of the $n \times n$ identity matrix is $n$.

(2) Since $\rho_\sigma$ has finite order, its eigenvalues $\lambda_1, \dots, \lambda_n$ have finite order as well. Hence they have absolute value 1. Hence

$$\begin{aligned}\overline{\chi(\sigma)} &= \overline{\mathrm{Tr}(\rho_\sigma)}\\ &= \sum \overline{\lambda_i}\\ &= \sum \lambda_i^{-1}\\ &= \sum \mathrm{Tr}(\rho_\sigma^{-1})\\ &= \sum \mathrm{Tr}(\rho_{\sigma^{-1}})\\ &= \chi(\sigma^{-1}).\end{aligned}$$

(3) We can also write this as $\chi(vu) = \chi(uv)$ with $u = \tau\sigma$ and $v = \tau^{-1}$. It then follows from

$$\mathrm{Tr}(ab) = \mathrm{Tr}(ba).$$

■

**Proposition 3.19** *Let $\rho^1 \colon G \to \mathrm{Aut}(V^1)$ and $\rho^2 \colon G \to \mathrm{Aut}(V^2)$ be two representations of $G$ and let $\chi_1$ and $\chi_2$ be their respective characters. Then:*

*(1) The character $\chi$ of the direct sum representation $V^1 \oplus V^2$ is $\chi_1 + \chi_2$.*

*(2) The character $\psi$ of the tensor product representation $V^1 \otimes V^2$ is $\chi_1 \cdot \chi_2$.*

Proof Write $\rho^1, \rho^2$ in matrix form: $R^1_\sigma, R^2_\sigma$. The representation $V_1 \oplus V_2$ is then given by the matrix

$$R_\sigma = \begin{pmatrix} R^1_\sigma & 0 \\ 0 & R^2_\sigma \end{pmatrix}.$$

Hence $\mathrm{Tr}(R_\sigma) = \mathrm{Tr}(R^1_\sigma) + \mathrm{Tr}(R^2_\sigma)$, that is $\chi(\sigma) = \chi_1(\sigma) + \chi_2(\sigma)$.

For (ii) we do a similar thing. Let $(e_{i_1})$ be a basis for $V^1$ and $(e_{i_2})$ be a basis for $V^2$. Let $(r_{i_1j_1}(\sigma)), (r_{i_2j_2}(\sigma))$ be the matrices of $\rho^1$ and $\rho^2$ with respect to these bases respectively. We then have

$$\begin{aligned}\rho^1_\sigma(e_{j_1}) &= \sum_{i_1} r_{i_1j_1}(s) e_{i_1},\\ \rho^2_\sigma(e_{j_2}) &= \sum_{i_2} r_{i_2j_2}(s) e_{i_2},\end{aligned}$$

which implies

$$\rho^1_\sigma \otimes \rho^2_\sigma(e_{j_1} \otimes e_{j_2}) = \sum_{i_1,i_2} r_{i_1j_1}(s) r_{i_2j_2}(s) e_{i_1} \otimes e_{i_2}$$

Hence

$$\begin{aligned}\mathrm{Tr}(\rho^1_\sigma \otimes \rho^2_\sigma) &= \sum_{i_1,i_2} r_{i_1i_2}(\sigma) r_{i_2i_2}(\sigma)\\ &= \chi_1(\sigma)\chi_2(\sigma).\end{aligned}$$

■

**Remark 3.20** If $\varphi$ and $\psi$ are complex-valued functions on $G$, we set

$$\langle\varphi, \psi\rangle = \frac{1}{\#G}\sum_{\tau\in G}\varphi(\tau^{-1})\psi(\tau) = \frac{1}{\#G}\sum_{\tau\in G}\varphi(\tau)\psi(\tau^{-1}).$$

We have $\langle\varphi, \psi\rangle = \langle\psi, \varphi\rangle$. Moreover, $\langle\varphi, \psi\rangle$ is linear in $\varphi$ and $\psi$. With this notation, corollary 3.15 and corollary 3.16 become, respectively,

$$\langle r_{i_2j_2}, r_{j_1i_1}\rangle = 0 \text{ and } \langle r_{i_2j_2}, r_{j_1i_1}\rangle = \frac{1}{n}\delta_{i_2i_1}\delta_{j_2j_1}.$$

**Definition 3.21** Let $\varphi$, $\psi$ be complex-valued functions on $G$. Define

$$(\varphi|\psi) = \frac{1}{\#G}\sum_{\tau\in G}\varphi(\tau)\overline{\psi(\tau)}.$$

This is a *scalar product*: it is is linear in $\varphi$, semi-linear in $\psi$, and $(\varphi|\varphi) > 0$ for all $\varphi \neq 0$.

**Definition 3.22** For a complex valued function $\psi$ on $G$ define $\psi^\vee(\tau) = \overline{\psi(\tau^{-1})}$.

**Remark 3.23** We then have $(\varphi|\psi) = \langle\varphi, \psi^\vee\rangle$. If $\chi$ is the character of a representation, we have $\chi = \chi^\vee$ by proposition 3.18 (2). Hence $(\varphi|\chi) = \langle\varphi, \chi\rangle$ for all $\varphi$ on $G$.

**Theorem 3.24** *(1) If $\chi$ is the character of an irreducible representation then $(\chi|\chi) = 1$ ($\chi$ has "norm 1").*

*(2) If $\chi$ and $\chi'$ are characters of non-isomorphic irreducible representations then $(\chi|\chi') = 0$ ($\chi$ and $\chi'$ are "orthogonal").*

Proof (1) Let $\rho$ be an irreducible representation with character $\chi$ and matrix representation $\rho_\tau = (r_{ij}(\tau))$. We have $\chi(\tau) = \sum r_{ii}(\tau)$. Hence

$$(\chi|\chi) = \langle\chi|\chi\rangle = \sum_{i,j}\langle r_{ii}, r_{jj}\rangle.$$

But by corollary 3.16 we have $\langle r_{ii}, r_{jj}\rangle = \delta_{ij}/n$. Hence

$$(\chi|\chi) = \left(\sum_{i,j}\delta_{ij}\right)/n = n/n = 1.$$

(2) Proved in the same way as (i), but by applying corollary 3.15 instead of corollary 3.16. ■

**Theorem 3.25** *Let $V$ be a linear representation of $G$, with character $\varphi$, and suppose $V$ decomposes into a direct sum of irreducible representations:*

$$V = W_1 \oplus \cdots \oplus W_k.$$

*Then, if $W$ is an irreducible representation with character $\chi$, the number of $W_i$ isomorphic to $W$ is equal to $(\varphi|\chi) = \langle\varphi|\chi\rangle$.*

Proof Let $\chi_i$ be the character of $W_i$. By proposition 3.19, we have

$$\varphi = \chi_1 + \cdots + \chi_k.$$

Hence $(\psi|\chi) = (\chi_1|\chi) + \cdots + (\chi_k|\chi)$. But by theorem 3.24 $(\chi_i|\chi)$ is equal to 1 or 0, depending on whether $W_i$ is or is not isomorphic to $W$. ■

**Corollary 3.26** *The number of $W_i$ isomorphic to $W$ is independent of the decomposition.*

Proof $(\varphi|\chi)$ is independent of the decomposition. ■

**Corollary 3.27** *Two representations with the same character are isomorphic.*

Proof Corollary 3.26 shows that they contain every irreducible representation the same number of times ■

Hence if $\chi_1, \dots, \chi_h$ are the distinct irreducible characters of $G$ and $W_1, \dots, W_h$ denote corresponding irreducible representations then each representation $V$ is isomorphic to a direct sum

$$V = m_1 W_1 \oplus \cdots \oplus m_k W_k \text{ with } m_i \text{ integers} \geq 0.$$

The character $\varphi$ of $V$ is equal to

$$m_1\chi_1 + \cdots + m_k\chi_k$$

and

$$m_i = (\varphi|\chi_i)$$

By orthogonality:

$$(\varphi|\varphi) = \sum_{i=1}^{k} m_i^2.$$

Hence

**Theorem 3.28** *If $\varphi$ is the character of a representation $V$, then $(\varphi|\varphi)$ is a positive integer, and $(\varphi|\varphi) = 1$ if and only if $\varphi$ is irreducible.*

Proof $\sum m_i^2$ is equal to 1 if and only if one of the $m_i$'s is 1 and the rest is 0.■

Let

$$\chi_1, \ldots, \chi_h$$

be the irreducible representations of a group $G$, of degrees

$$n_1, \ldots, n_k.$$

. (Then $n_i = \chi_i(1)$.) Let $\rho\colon G \to \mathrm{Aut}(R)$ be the regular representation. Then $\rho_\sigma(e_\tau) = e_{\sigma\tau}$, hence the diagonal of the matrix representation of $\rho_\sigma$ consists of zeroes if $\sigma \neq 1$ and it consists of 1's if $\sigma = 1$. Hence $\mathrm{Tr}(\rho_\sigma) = 0$ if $\sigma \neq 1$ and $\mathrm{Tr}(\rho_1) = \dim R = \#G$. Hence we have

**Proposition 3.29** *The character $r_G$ of the regular representation is given by*

$$r_G(1) = \#G,$$
$$r_G(\sigma) = 0 \textit{ if } \sigma \neq 1.$$

**Corollary 3.30** *Every iredducible representation $W_i$ is contained in the regular representation with multiplicity equal to $n_i$.*

Proof By theorem 3.25 this is equal to

$$\begin{aligned}\langle r_G, \chi_i \rangle &= \frac{1}{\#G} \sum_{\sigma \in G} r_G(\sigma^{-1}) \chi_i(\sigma) \\ &= \frac{1}{\#G} \#G \chi_i(1) \\ &= n_i.\end{aligned}$$

■

**Corollary 3.31** *A group has a finite number of non-isomorphic irreducible representations. Consequently it has also a finite number of irreducible characters.*

**Corollary 3.32** *(a) The degrees satisfy*

$$\sum_{i=1}^{k} n_i^2 = \#G.$$

*(b) If $\sigma \neq 1$ then*

$$\sum_{i=1}^{k} n_i \chi_i(\sigma) = 0$$

Proof By corollary 3.30:

$$r_G(\sigma) = \sum n_i \chi_i(\sigma).$$

Taking $\sigma = 1$ we get (a), taking $\sigma \neq 1$ we get (b). ■

**Definition 3.33** A function $f\colon G \to \mathbf{C}$ is called a **class function** if it is constant on conjugacy classes. Equivalently it factors through $G/\operatorname{Cl} G$, where $\operatorname{Cl} G$ denotes the set of conjugacy classes of $G$.

**Proposition 3.34** *Let $f$ be a class function, $\rho$ a representation. Put $\rho_f = \sum_{\tau \in G} f(\tau)\rho_\tau$. If $\rho$ is irreducible, of degree $n$ and with character $\chi$, then $\rho_f$ is a homothety of ratio*

$$\begin{aligned}\lambda &= \frac{1}{n}\sum_{\tau \in G} f(\tau)\chi(\tau)\\ &= \frac{\#G}{n}(f|\chi^*).\end{aligned}$$

Proof We have

$$\begin{aligned}\rho_\sigma^{-1}\rho_f\rho_\sigma &= \sum_{\tau \in G} f(\tau)\rho_\sigma^{-1}\rho_\tau\rho_\sigma\\ &= \sum_{\tau \in G} f(\tau)\rho_{\sigma^{-1}\tau\sigma}.\end{aligned}$$

Putting $u = \sigma^{-1}\tau\sigma$, this becomes:

$$\begin{aligned}\rho_\sigma^{-1}\rho_f\rho_\sigma &= \sum_{u \in G} f(\sigma u \sigma^{-1})\rho_u\\ &= \sum_{u \in G} f(u)\rho_u\\ &= \rho_f.\end{aligned}$$

So we have $\rho_f\rho_\sigma = \rho_\sigma\rho_f$. By Schur's Lemma, this shows that $\rho_f$ is a homothety $\lambda$. We have $\operatorname{Tr}\lambda = n\lambda$ and

$$\begin{aligned}\operatorname{Tr}\rho_f &= \sum_{\tau \in G} f(\tau)\operatorname{Tr}(\rho_\tau)\\ &= \sum_{\tau \in G} f(\tau)\chi(\tau).\end{aligned}$$

Hence

$$\begin{aligned}\lambda &= \frac{1}{n}\sum_{\tau \in G} f(\tau)\chi(\tau)\\ &= \frac{\#G}{n}(f|\overline{\chi})\end{aligned}$$

■

**Definition 3.35** *$H$ is the set of class functions. It is a vector space over $\mathbf{C}$.*

**Theorem 3.36** *The irreducible characters $\chi_1, \dots, \chi_h$ form an orthonormal basis of $H$.*

Proof Theorem 3.24 shows that the $\chi_i$ form an orthonormal set. It remains to show that they generate $H$. It is straightforward to verify that the $\overline{\chi_i}$ are also the irreducible characters . Hence it is enough to show that every $f \in H$ that is orthogonal to all the $\overline{\chi_i}$ is zero.

For $\rho$ a representation of $G$, put

$$\rho_f = \sum_{\tau \in G} f(\tau)\rho_\tau.$$

as in the proof of proposition 3.34. Since $f$ is orthogonal to all $\overline{\chi_i}$ proposition 3.34 shows that $\rho_f = 0$ if $\rho$ is irreducible. Every representation is the sum of irreducible representations, hence $\rho_f = 0$ for every representation. Apply this to the regular representation $R$. Compute

$$\begin{aligned} \rho_f e_1 &= \sum_{\tau \in G} f(\tau)\rho_\tau e_1 \\ &= \sum_{\tau \in G} f(\tau) e_\tau. \end{aligned}$$

Since $\rho_f = 0$, we have $\rho_f e_1 = 0$, hence $f(\tau) = 0$ for all $\tau \in G$. Hence $f = 0$. ■

**Theorem 3.37** *The number of irreducible representations of $G$ is equal to the number of conjugacy classes of $G$.*

Proof Every class function is determined by its values on the conjugacy classes, and for those values there is a free choice. Hence the number of conjugacy classes is equal to the $\mathbf{C}$-dimension of the space of class-functions.

But theorem 3.36 shows that the $\mathbf{C}$-dimension of the space of class functions is also equal to the number of irreducible characters. This is equal to the number of irreducible representations. Hence the number of conjugacy classes is equal to the number of irreducible representations. ■

**Proposition 3.38** *Let $s \in G$, $c(s)$ the cardinality of the conjugacy class of $s$, $\chi_1, \dots, \chi_h$ the irreducible characters of $G$. Then*

*(a) $\sum_{i=1}^h \chi_i(s)^* \chi(s) = \frac{\#G}{c(s)}$.*

*(b) For $t$ not conjugate to $s$, we have $\sum_{i=1}^h \chi_i(s)^* \chi_i(t) = 0$.*

Proof Let $\mathbf{1}_s$ be the indicator function of the class of $s$. This is a class function. By theorem 3.36 it can be written

$$\mathbf{1}_s = \sum_{i=1}^h \lambda_i \chi_i,$$

with $\lambda_i = (\mathbf{1}_s|\chi_i) = c(s)/\#G\chi^*(s)$. For each $t \in G$ we then have

$$\mathbf{1}_s(t) = \frac{c(s)}{\#G}\sum_{i=1}^{h} \chi_i(s)^*\chi_i(t).$$

This gives (a) if $t = s$ and (b) if $t$ is not conjugate to $s$. ■

**Theorem 3.39** *Let $G$ be a group. The following are equivalent:*

*(i) $G$ is abelian.*

*(ii) All irreducible representations of $G$ have degree 1.*

Proof Let $n_1, \dots, n_h$ be the degrees of the irreducible representations. We know that $h$ is the number of conjugacy classes by theorem 3.37, and that $\#G = n_1^2 + \cdots n_h^2$ by corollary 3.32. Hence $\#G$ is equal to $h$ if and only if all $n_i = 1$, hence $G$ is abelian if and only if every representation is of degree 1. ■

Let $\rho\colon G \to \mathrm{Aut}(V)$ be a representation, $H < G$, $\rho_H$ the restriction of $\rho$ to $H$. Let $W$ be a subrepresentation of $\rho_H$ (i.e. $W$ is a subpace of $V$ and $\rho_t W = W$ for all $t \in H$). Denote this representation by $\vartheta\colon H \to \mathrm{Aut}(W)$. Let $s \in G$. Then $\rho_s W$ only depends on the coset $sH$. Thus for a coset $\sigma$ can define $W_\sigma$ as $\rho_s W$ with any $s \in \sigma$. The $W_\sigma$ are mapped to one another by the $\rho_s$, $s \in G$. Hence their sum $\sum_{\sigma \in G/H} W_\sigma$ is a subrepresentation of $V$.

**Definition 3.40** We say that the representation $\rho$ of $G$ in $V$ is induced by $\vartheta$ from $H$ in $W$ if $V$ is equal to the sum of the $W_\sigma$ ($\sigma \in G/H$) and if this sum is direct.

**Remark 3.41** This means in particular that $\dim V = (G : H) \dim W$.

Recall that $G$-representations correspond to $\mathbf{C}[G]$-moduls. Let $V$ be a $\mathbf{C}[G]$-module, $W$ a sub-$\mathbf{C}[H]$-module. Then $V$ is induced by $W$ if and only if

$$V = \bigoplus_{\sigma \in G/H} \sigma W.$$

(Where $\sigma W = sW$ for some $s \in \sigma$, which is independent of the choice made.)

**Proposition 3.42** *$V$ is induced by $W$ if and only if the homomorphism*

$$\mathbf{C}[G] \otimes_{\mathbf{C}[H]} W \to V$$

*is an isomorphism.*

Proof Let $R$ be a system of representatives of $G/H$. Then

$$\mathbf{C}[G] = \bigoplus_{s \in R} s\mathbf{C}[H],$$

hence

$$\begin{aligned}\mathbf{C}[G] \otimes_{\mathbf{C}[H]} W &= \bigoplus_{s\in R} s\mathbf{C}[H]W \\ &= \bigoplus_{s\in R} sW. \end{aligned}$$ ■

**Remark 3.43** This makes it obvious that the induced representation always exists and is unique: it is

$$\mathbf{C}[G] \otimes_{\mathbf{C}[H]} W.$$

We will denote it by $\operatorname{Ind}_H^G(W)$ or $\operatorname{Ind}(W)$.

**Remark 3.44** If $E$ is a $\mathbf{C}[G]$-module we have a canonical isomorphism

$$\operatorname{Hom}_{\mathbf{C}[H]}(W, E) \cong \operatorname{Hom}_{\mathbf{C}[G]}(\operatorname{Ind} W, E)$$

where both Hom-sets are considered as $\mathbf{C}$-vector spaces, and $E$ on the left hand side is considered as a $\mathbf{C}[H]$-module.

**Remark 3.45** By associativity of the tensor product this also shows that induction is transitive: if $H < G < K$ and $W$ is a sub-$\mathbf{C}[H]$-module then

$$\begin{aligned}\operatorname{Ind}_G^K(\operatorname{Ind}_H^G(W)) &= \mathbf{C}[K] \otimes_{\mathbf{C}[H]} \big(\mathbf{C}[G] \otimes_{\mathbf{C}[H]} W\big) \\ &\cong \big(\mathbf{C}[K] \otimes_{\mathbf{C}[H]} \mathbf{C}[G]\big) \otimes_{\mathbf{C}[H]} W \\ &\cong \mathbf{C}[K] \otimes_{\mathbf{C}[H]} W \\ &= \operatorname{Ind}_H^K(W).\end{aligned}$$

**Proposition 3.46** *Let $V$ be a $\mathbf{C}[G]$-module, and suppose $V$ decomposes as $V = \bigoplus_{i\in I} W_i$. Suppose furthermore that the $W_i$ are transitively permuted by $G$. Let $i_0 \in I$, $W = W_{i_0}$. Let $H$ be the stabilizer of $W$ in $G$.*

*Then $W$ is stable under $H$ and the $\mathbf{C}[G]$-module $V$ is induced by the $\mathbf{C}[H]$-module $W$.*

Proof Let $R$ be a system of representatives of $G/H$. $W$ is stable under $H$ by definition of the stabilizer. By the orbit-stabilizer theorem we have $\#(G/H) = \#I$. Hence for every $i \in I$ there is a unique $s \in R$ such that $sW = W_i$. This shows that $V = \bigoplus_{i\in I} W_i = \bigoplus_{s\in R} sW$. ■

**Remark 3.47** In order to apply proposition 3.46 to an irreducible representation $V$ it is enough to check that the $W_i$ are permuted among themselves: transitivity follows since each orbit defines a subrepresentation.

**Theorem 3.48** *Let $H < G$, $(W, \vartheta)$ a $H$-representation, $(V, \rho)$ the $G$-representation induced by $W$, $\chi_\vartheta$ and $\chi_\rho$ their respective characters. Let $R$ be a system of representatives of $G/H$. Then for each $u \in G$:*

$$\chi_\rho(u) = \sum_{\substack{r\in R\\ r^{-1}ur\in H}} \chi_\vartheta(r^{-1}ur) = \frac{1}{\#H} \sum_{\substack{s\in G\\ s^{-1}us\in H}} \chi_\vartheta(s^{-1}us).$$

We have

$$V = \bigoplus_{r \in R} \rho_r W.$$

$\rho_u$ permutes the $\rho_r W$ among themselves: if we write $ur = r_u t$ with $r_u \in R$ and $t \in H$ we see that $\rho_u \rho_r W = \rho_{r_u} W$. To determine $\chi_\rho(u) = \mathrm{Tr}_V(\rho_U)$, use a basis of $V$ which is the union of bases of the $\rho_r W$. The indices such that $r_u \neq r$ give zero diagonal terms. The others give the trace of $\rho_u$ on $\rho_r W$.

Denoting by $R_u$ the $r \in R$ such that $r_u = r$ we obtain

$$\chi_\rho(u) = \sum_{r \in R_u} \mathrm{Tr}_{\rho_r W}(\rho_{u,r})$$

where $\rho_{u,r}$ denotes the restriction of $\rho_u$ to $\rho_r W$. Observe that

$$\begin{aligned} r \in R_u &\iff ur = rt \text{ with } t \in H \\ &\iff r^{-1}ur \in H. \end{aligned}$$

We have, with $t = r^{-1}ur$,

$$\begin{aligned} \rho_{u,r} &= \rho_r^{-1} \circ \rho_t \rho_r \\ &= \rho_r^{-1} \vartheta_t \rho_r, \end{aligned}$$

hence $\mathrm{Tr}_{\rho_r W}(\rho_{u,r}) = \mathrm{Tr}_W(\vartheta_t) = \chi_\vartheta(t) = \chi_\vartheta(r^{-1}ur)$. Hence:

$$\chi_\rho(u) = \sum_{r \in R_u} \chi_\vartheta(r^{-1}ur).$$

The second formula follows from the first.

**Definition 3.49** Let $H < G$, $f$ a class function on $H$. Define $f'$ on $G$ by

$$f'(s) = \frac{1}{\#H} \sum_{\substack{t \in G \\ t^{-1}st \in H}} f(t^{-1}st).$$

We say that $f'$ is **induced** by $f$ and denote it by $\mathrm{Ind}_H^G(f)$ or $\mathrm{Ind}(f)$.

**Proposition 3.50** *(i)* $\mathrm{Ind}(f)$ *is a class function on* $G$.

*(ii) If* $f = \chi_\vartheta$ *where* $(W, \vartheta)$ *is a representation of* $H$ *then* $\mathrm{Ind}(\chi_\vartheta)$ *is the character of* $\mathrm{Ind}(W)$.

Proof (ii) was the content of theorem 3.48. (i) follows from direct calculation or from (ii) and the observation that every class function is a linear combination of characters. ∎

**Definition 3.51** If $V_1$ and $V_2$ are $\mathbf{C}[G]$-modules, we set

$$\langle V_1, V_2 \rangle_G = \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}[G]}(V_1, V_2).$$

**Lemma 3.52** *If $\varphi_1$ and $\varphi_2$ are the characters of $V_1$ and $V_2$ we have*

$$\langle \varphi_1, \varphi_2 \rangle_G = \langle V_1, V_2 \rangle_G.$$

Proof Decomposing $V_1$ and $V_2$ into direct sums, we may assume that $V_1$ and $V_2$ are irreducible, in which case the lemma follows from theorem 3.24 and Schur's lemma. ■

If $\varphi$ (resp. $V$) is a function on $G$ (resp. a representation of $G$), we denote by $\operatorname{Res}\varphi$ (resp. $\operatorname{Res} V$) its restriction to the subgroup $H$.

**Theorem 3.53 (Frobenius Reciprocity)** *Let $\psi$ be a class function on $H$, $\varphi$ a class function on $G$. Then*

$$\langle \psi, \operatorname{Res}\varphi \rangle_H = \langle \operatorname{Ind}\psi, \varphi \rangle_G.$$

Proof Every class function is a linear combination of characters, hence we can assume $\psi$ is the character of some $\mathbf{C}[H]$-module $W$ and $\varphi$ is the character of some $\mathbf{C}[G]$-module $E$. Because of lemma 3.52 and proposition 3.50 it is enough to show that

$$\langle W, \operatorname{Res} E \rangle_H = \langle \operatorname{Ind} W, E \rangle_G,$$

i.e.

$$\dim_{\mathbf{C}} \operatorname{Hom}_{\mathbf{C}[H]}(W, \operatorname{Res} E) = \dim_{\mathbf{C}} \operatorname{Hom}_{\mathbf{C}[G]}(\operatorname{Ind} W, E),$$

which follows from remark 3.44. ■

**Remark 3.54** Theorem 3.53 expresses that Res and Ind are adjoints.

**Remark 3.55** Instead of $\langle\ ,\ \rangle$ we can use $(\ |\ )$ to get the same formula:

$$(\psi | \operatorname{Res}\varphi)_H = (\operatorname{Ind}\psi | \varphi)_G.$$

Let $H, K < G$, and consider a representation $\rho\colon H \to \operatorname{Aut}(W)$. Let $V = \operatorname{Ind}_H^G(W)$. We shall determine $\operatorname{Res}_K(V)$. Note that $K \times H$ acts on $G$ by $(k, h) \cdot g = kgh^{-1}$. Choose a set $S$ of representatives of the orbits $KgH$, $g \in G$: $G$ is then the disjoint union

$$\bigcup_{s \in S} KsH.$$

For $s \in S$, let $H_s = sHs^{-1} \cap K$, which is a subgroup of $K$. Set

$$\rho^s(x) = \rho(s^{-1}xs), \text{ for } x \in H.$$

We thus obtain a homomorphism $\rho^s\colon H_s \to \operatorname{Aut}(W)$, hence a representation of $H_s$, denoted $W_s$. Since $H_s < K$, $\operatorname{Ind}_{H_s}^K(W_s)$ is defined.

**Proposition 3.56 (Mackey's Formula)** *Let $S$ be a system of representatives of $K\backslash G/H$. Then*

$$\operatorname{Res}_K \operatorname{Ind}_H^G(W) \cong \bigoplus_{s\in S} \operatorname{Ind}_{H_s}^K(W_s).$$

Proof Let $S$ be a system of representatives of $K\backslash G/H$. Then $V = \oplus_{x\in R} xW$. Let $V(s)$ be the subspace generated by the $xW$, for $x \in KsH$. Then every $V(s)$ is spanned by some of the $xW$, and these spanning sets are mutually disjoint for different $s$. Hence

$$V = \bigoplus_{s\in S} V(s).$$

The $V(s)$ are stable under $K$. It remains to show that $V(s)$ is $\mathbf{C}[K]$-isomorphic to $\operatorname{Ind}_{H_s}^K(W_s)$. But the subgroup of $K$ consisting of those $x$ such that $x(sW) = sw$ is equal to those $x \in K$ such that

$$\begin{gathered} s^{-1}xsW = W \\ \Longleftrightarrow \\ s^{-1}xs \in H \\ \Longleftrightarrow \\ x \in sHs^{-1}. \end{gathered}$$

Hence this subgroup is equal to $sHs^{-1} \cap K = H_s$. Hence we have

$$V(s) \cong \bigoplus_{x\in K/H_s} x(sW),$$

hence $V(s) = \operatorname{Ind}_{H_s}^K(sW)$. It remains to show that $sW$ is $\mathbf{C}[H_s]$-ismorphic to $W_s$. But this is true: an isomorphism is given by $s\colon W_s \to sW\colon w \mapsto sw$. ■

**Theorem 3.57 (Artin's Induction Theorem)** *Let $G$ be a finite group, $\rho$ a $G$-representation. Then:*

*For some $n \geq 1$, there exists cyclic subgroups $H_i, H'_j < G$ and 1-dimensional representations $\psi_i, \psi'_i$ of $H_i, H'_j$ respectively such that*

$$\rho^{\oplus n} \oplus \bigoplus_i \operatorname{Ind}_{H_i}^G \psi_i \cong \bigoplus_J \operatorname{Ind}_{H'_j}^G \psi'_j.$$

*If $\langle \rho, \mathbf{1}\rangle = 0$, then all $\psi_i, \psi'_j$ can be chosen to be non-trivial.*

Proof If $\tau$ is a $G$-representation write $\chi_\tau$ for its character.

Let $V$ be the $\mathbf{Q}$-vector space spanned by the characters of $G$. Let $W$ be the subspace spanned by $\chi_{\operatorname{Ind}_H^G \tau}$ for all cyclic $H < G$ and 1-dimensional $H$-representations $\tau$ (= all irreducible $H$-representations as $H$ is abelian). It suffices to show $V = W$ for then

$$\chi_\rho = \sum_m \lambda_m \chi_{\operatorname{Ind}_H^G \tau_m} \qquad \lambda_m \in \mathbf{Q},$$

hence for some $n > 0$

$$n\chi_\rho = \sum_m k_m \chi_{\mathrm{Ind}_H^G \tau_m} \qquad k_m \in \mathbf{Z},$$

hence

$$n\chi_\rho + \sum_{\substack{i \\ k_i<0}} k_i \chi_{\mathrm{Ind}_H^G \tau_i} = \sum_{\substack{j \\ k_j>0}} k_j \chi_{\mathrm{Ind}_H^G \tau_j},$$

and as the character of a representation determines the representation and character of direct sums is the sum of characters, we are done.

Hence suppose that $\psi \in W^\perp$, i.e. $\langle \psi, \chi_{\mathrm{Ind}_H^G \tau \rangle} \rangle = 0$ for all cyclic $H < G$ and 1-dimensional $H$-representations $\tau$. By Frobenius reciprocity:

$$\langle \mathrm{Res}_H^G \psi, \chi_\tau \rangle = 0$$

for all irreducible representations $\tau$ of $H$. Hence: $\mathrm{Res}_H^G \psi = 0$. In particular, taking $H = \langle g \rangle$ shows that $\psi(g) = 0$. This holds for all $g \in G$, hence $\psi = 0$, hence $W^\perp = 0$, hence $V = W$.

For the second claim, take $W$ to be generated by the $\chi_{\mathrm{Ind}_H^G \tau}$ with $H$ cyclic and $\tau \neq \mathbf{1}$ 1-dimensional. It suffices to check that every $\psi \in W^\perp$ is a multiple of the trivial character, for the trivial character does not occur in the decomposition of $\chi_\rho$ by $\langle \rho, \mathbf{1} \rangle = 0$. By Frobenius reciprocity:

$$\langle \mathrm{Res}_H^G \psi, \tau \rangle_H = 0$$

for all $H$ cyclic, $\tau \neq \mathbf{1}$ 1-dimensional, hence $\mathrm{Res}_H^G \psi$ is a multiple of $\mathbf{1}_H$. Taking $H = \langle g \rangle$ shows that $\psi(g) = \psi(e)$ (where $e$ is the identity of $G$). This is true for all $g \in G$, hence $\psi$ is a multiple of $\mathbf{1}_G$. ■

# Chapter 4

# $L$-Series

## 4.1 Dirichlet $L$-series

In this section we define zeta functions and $L$ functions and derive properties that we will need later, namely that $L$ functions can be extended analytically to a complex right-half plane including 1 to a function which is regular everywhere except possibly in 1 if it is the $L$-function of the trivial character. In that case, the extension has a simple pole in 1. The material is from Lang [9, chapter VIII].

**Proposition 4.1 (Summation by Parts, Abel's Lemma)** *Let*

$$(a_n)_n, (b_n)_n$$

*be sequences of complex numbers. Let*

$$\begin{aligned} A_n &= a_1 + \cdots + a_n, \\ B_n &= b_1 + \cdots + b_n \end{aligned}$$

*be their partial sums. Then*

$$\sum_{n=1}^{N-1} a_n b_n = A_N b_N + \sum_{n=1}^{N-1} A_n(b_n - b_{n+1})$$

Proof

$$\begin{aligned}\sum_{n=1}^{N-1} A_n(b_n - b_{n+1}) &= \sum_{n=1}^{N-1}\sum_{j=1}^{n} a_j(b_n - b_{n+1}) \\ &= \sum_{j=1}^{N-1}\sum_{n=j}^{N-1} a_j(b_n - b_{n+1}) \\ &= \sum_{j=1}^{N-1} a_j(b_j - b_N) \\ &= \sum_{n=1}^{N} a_n b_n - a_N b_N - A_{N-1} b_N \\ &= \sum_{n=1}^{N} a_n b_n - A_N b_N. \end{aligned}$$ ■

**Definition 4.2** A **Dirichlet series** is a series of the form

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where $(a_n)_n$ is a sequence of complex numbers and $s$ is a complex variable. We write $s = \sigma + it$ with $\sigma, t \in \mathbf{R}$.

**Theorem 4.3** *If a Dirichlet series $\sum_n a_n/n^s$ converges for some $s = s_0$, then it converges for any $s$ with* $\mathrm{Re}(s) > \sigma_0 = \mathrm{Re}(s_0)$*, uniformly on any compact subset of this region.*

Proof Convergence follows by comparison with $\sum_n a_n/n^{s_0}$. (Note that for all complex $s$ we have $|n^s| = n^\sigma$.)

To see why the convergence is uniform on compact subsets, write $n = n^{s_0} n^{s-s_0}$, $P_n(s_0) = \sum_{m=1}^{n} a_m/m^{s_0}$. We will give a uniform bound for the tail. Let $m < n$. Consider the $m$-th and $n$-th partial sums of the series

$$\sum \frac{a_n}{n^{s_0}} \frac{1}{n^{s-s_0}},$$

sum these by parts, and subtract the $n$-th partial sum from the $m$-th, to get

$$\sum_{k=m+1}^{n} \frac{a_k}{k^{s_0}} \frac{1}{k^{s-s_0}} = \frac{P_n(s_0)}{n^{s-s_0}} \quad + \sum_{k=m+1}^{n-1} P_k(s_0)\left(\frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}}\right) - \frac{P_m(s_0)}{(m+1)^{s-s_0}}.$$

Letting $n \to \infty$ we obtain the tail:

$$\sum_{k=m+1}^{\infty} \frac{a_k}{k^{s_0}} \frac{1}{k^{s-s_0}} = \sum_{k=m+1}^{\infty} P_k(s_0) \left( \frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}} \right) - \frac{P_m(s_0)}{(m+1)^{s-s_0}}.$$

Letting $m$ be large enough we can make the second term smaller than $\epsilon$, uniformly in $s$ (since it does not depend on $s$). Also, by letting $m$ be large enough, we can bound $P_k(s_0)$ by $\epsilon$ (since the partial sums converge at $s = s_0$). Denote $s = \mathrm{Re}(\sigma)$ and recall that $s_0 = \mathrm{Re}(\sigma_0)$. We can estimate

$$\begin{aligned}
\left| \sum_{k=m+1}^{\infty} P_k(s_0) \left( \frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}} \right) \right| &\leq \epsilon \sum_{k=m+1}^{\infty} \left| \frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}} \right| \\
&= \epsilon \sum_{k=m+1}^{\infty} \left| (s - s_0) \int_k^{k+1} \frac{1}{x^{s-s_0+1}} \, dx \right| \\
&\leq \epsilon |s - s_0| \int_1^{\infty} \frac{1}{x^{\sigma - \sigma_0 + 1}} \, dx \\
&= \epsilon \frac{|s - s_0|}{|\sigma - \sigma_0|},
\end{aligned}$$

and the factor after the $\epsilon$ is bounded on compact subsets. ■

**Definition 4.4** Assuming that a Dirichlet series converges for some $s$, if $\sigma_0$ is the smallest real number such that the series converges for $\mathrm{Re}(s) > \sigma_0$, then we call $\sigma_0$ the **abscissa of convergence**.

**Theorem 4.5** *Assume there exists numbers $C$ and $\sigma_1 > 0$ such that*

$$|A_n| = |a_1 + \ldots + a_n| \leq C n^{\sigma_1}$$

*for all $n$. Then the abscissa of convergence of $\sum a_n / n^s$ is $\leq \sigma_1$.*

PROOF Let $\delta > 0$ and let $\mathrm{Re}(s) \geq \sigma_1 + \delta$. Sum by parts to obtain for the difference of the partial sums:

$$\begin{aligned}
P_n(s) - P_m(s) &= A_n \frac{1}{n^s} + \sum_{k=m+1}^{n-1} A_k \left[ \frac{1}{k^s} - \frac{1}{(k+1)^s} \right] - A_m \frac{1}{m^s} \\
&= A_n \frac{1}{n^s} + \sum_{k=m+1}^{n-1} A_k s \int_k^{k+1} \frac{1}{x^{s+1}} \, dx - A_m \frac{1}{m^s}.
\end{aligned}$$

The left and right term can be bounded by $C/n^{\delta}$ and $C/m^{\delta}$ respectively. For the middle term we have:

$$\begin{aligned}
&\left|A_k s \int_k^{k+1} \frac{1}{x^{s+1}}\ dx\right| \\
&= \left|C \int_k^{k+1} \frac{k^{\sigma_1}}{x^{\sigma+1}}\ dx\right| \\
&= \left|C \int_k^{k+1} \frac{x^{\sigma_1}}{x^{\sigma+1}}\ dx\right| \\
&= \left|C \int_k^{k+1} \frac{1}{x^{\sigma-\sigma_1+1}}\ dx\right|.
\end{aligned}$$

Summing this from $k = m+1$ to $\infty$ yields

$$C \frac{1}{\sigma - \sigma_1} \frac{1}{(m+1)^{\sigma-\sigma_1}}.$$

Hence:

$$|P_n(s) - P_m(s)| \leq C/n^\delta + C \frac{|s|}{\delta(m+1)^\delta} + C/m^\delta.$$

This is small if we let $m$ go to $\infty$. ■

Let

$$\zeta(s) = \sum_n \frac{1}{n^s}.$$

This is the **Riemann zeta function**. Theorem 4.5 shows that $\zeta$ is analytic in $s$ for $\mathrm{Re}(s) > 1$ (with $\sigma_1 = 1$). For real $s > 1$ we have

$$\frac{1}{s-1} = \int_1^\infty \frac{1}{x^s}\ dx \leq \zeta(s) \leq 1 + \frac{1}{s-1}.$$

The first inequality follows from comparing the integral with Riemann sums, the second inequality follows from drawing a picture. It is based on the principle that for a positive strictly monotonic decreasing integrable function $f$ we have

$$\sum_{k=1}^\infty f(k) \leq \int_1^\infty f(x)\, dx + f(1).$$

Hence for real $s > 1$ we have

$$1 \leq (s-1)\zeta(s) \leq s.$$

We shall show that $\zeta$ can be extended analytically to all $s$ with $\mathrm{Re}(s) > 1$, and that it is analytic every except possibly at $s = 1$. The preceeding estimate implies it has a simple pole there, with residue 1.

Consider the alternating $\zeta$-function:

$$\zeta_2(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \cdots .$$

The partial sums of the coefficients are 0 and 1, hence bounded. Theorem 4.5 shows that $\zeta_2(s)$ is analytic for $\mathrm{Re}(s) > 0$. But

$$2 \cdot \underbrace{\frac{1}{2^s}\zeta(s)}_{\substack{\text{even terms}\\ \text{of } \zeta}} + \underbrace{\zeta_2(s)}_{\substack{\text{+ odd terms}\\ \text{- even terms}}} = \zeta(s),$$

and therefore

$$\zeta_2(s) = \left(1 - \frac{1}{2^{s-1}}\right)\zeta(s).$$

This gives an analytic continuation of $\zeta$ to the line $\sigma = 0$.

We must still investigate the poles. Consider the functions

$$\zeta_r(s) = \frac{1}{1^s} + \frac{1}{2^s} + \cdots \frac{1}{(r-1)^s} - \frac{(r-1)}{r^s} + \frac{1}{(r+1)^s} + \cdots$$

with $r = 2, 3, \ldots$. Just as with $r = 2$, we see that the partial sums are bounded by $r$, hence $\zeta_r(s)$ is analytic for $\mathrm{Re}(s) > 0$. Again, we have

$$r\frac{1}{r^s}\zeta(s) + \zeta_r(s) = \zeta(s),$$

hence

$$\zeta(s) = \frac{\zeta_r(s)}{1 - \frac{1}{r^{s-1}}}.$$

From $r = 2$ we see that the only possible poles occur when $2^{s-1} = 1$, or, equivalently, when

$$s = \frac{2\pi i n}{\log 2} + 1.$$

From the expression with $\zeta_3$ we see that for a pole

$$s = \frac{2\pi i m}{\log 3} + 1,$$

hence $2^m = 3^n$, which implies $n = m = 0$, hence $s = 1$. Hence we have shown:

**Theorem 4.6** *$\zeta(s)$ defines an analytic function for $\mathrm{Re}(s) > 0$, except for a simple pole at $s = 1$. If $\delta > 0$, then series $\sum 1/n^s$ for $\zeta(s)$ converges absolutely and uniformly on compact sets in the region $\mathrm{Re}(s) \geq 1 + \delta$.*

**Theorem 4.7** *Let $(a_n)_n$ be a sequence of complex numbers, with partial sums $A_n$. Let $0 \leq \sigma_1 < 1$, and assume that there is a complex number $\rho$, and $C > 0$ such that for all $n$ we have*

$$|A_n - n\rho| \leq Cn^{\sigma_1},$$

*or in other words $A_n = n\rho + O(n^{\sigma_1})$. Then the function*

$$f(s) = \sum a_n/n^s$$

*defined by these series for $\mathrm{Re}(s) > 1$ has an analytic continuation to $\mathrm{Re}(s) > \sigma_1$ where it is analytic except for a simple pole with resiude $\rho$ at $s = 1$.*

For the definition of characters and the $\mathfrak{c}$-ideal class group, see chapter 3 and section 2.1 respectively.

Proof Apply theorem 4.6 and theorem 4.5 to the function $f(s) - \rho\zeta(s)$. ■

**Definition 4.8** Let $K$ be a number field of degree $N$. Let $I(\mathfrak{c})/P_\mathfrak{c}$ be its $\mathfrak{c}$-class group. Let $\chi$ be a character of $I(\mathfrak{c})/P_\mathfrak{c}$. Then $\chi$ also induces a character on $I(\mathfrak{c})$ via the quotient map $I(\mathfrak{c}) \to I(\mathfrak{c})/P_\mathfrak{c}$. Denote this character also by $\chi$. Define the **$L_\mathfrak{c}$-series** of $\chi$ by

$$L_\mathfrak{c}(\chi, s) = \sum_{(\mathfrak{a},\mathfrak{c})=1} \frac{\chi(\mathfrak{a})}{\mathbf{N}\mathfrak{a}^s}$$

with $s$ a complex variable and the sum is over the integral ideals $\mathfrak{a} \in I$.

**Proposition 4.9** *The $L_\mathfrak{c}$-series converge on the half plane $\mathrm{Re}(s) > 1$.*

Proof Note that the $L_\mathfrak{c}$-series are a Dirichlet series with

$$a_n = \sum_{\substack{(\mathfrak{a},\mathfrak{c})=1 \\ \mathbf{N}\mathfrak{a}=n}} \chi(\mathfrak{a}),$$

Let $A_n$ denote the partial sum. We have

$$\begin{aligned}
&\#\{\mathfrak{a} : \mathfrak{a} \text{ integral ideal in } I(\mathfrak{c}) \text{ of norm} \leq n\} \\
&= \sum_{\mathcal{R} \in I(\mathfrak{c})/P_\mathfrak{c}} \{\text{integral } \mathfrak{a} \in \mathcal{R} \text{ of norm} \leq n\} \\
&= \sum_{\mathcal{R} \in I(\mathfrak{c})/P_\mathfrak{c}} j(\mathcal{R}, n) \\
&\overset{2.33}{=} \sum_{\mathcal{R} \in I(\mathfrak{c})/P_\mathfrak{c}} \left(\rho_\mathfrak{c} n + O_\mathcal{R}(t^{1-1/N})\right) \\
&= h_\mathfrak{c}\rho_\mathfrak{c} n + O(t^{1-1/N}),
\end{aligned}$$

where the subscript $\mathcal{R}$ of the $O$ denotes that the constant there in principle could depend on $\mathcal{R}$. In the last line this $\mathcal{R}$ is gone, because we can just take the maximum of all the constants for all $\mathcal{R}$. Hence we get

$$\begin{aligned}|A_n| &= \left|\sum_{\substack{(\mathfrak{a},\mathfrak{c})=1\\ \mathbf{N}\mathfrak{a}\le n}} \chi(\mathfrak{a})\right| \\ &= \sum_{\substack{(\mathfrak{a},\mathfrak{c})=1\\ \mathbf{N}\mathfrak{a}\le n}} |\chi(\mathfrak{a})| \\ &= \sum_{\substack{(\mathfrak{a},\mathfrak{c})=1\\ \mathbf{N}\mathfrak{a}\le n}} |1| \qquad (4.1) \\ &= h_{\mathfrak{c}}\rho_{\mathfrak{c}} n + O(n^{1-1/N}) \\ &\le Cn\end{aligned}$$

for suitable $C > 0$, because the sum on line (4.1) is equal to the number of ideals prime to $\mathfrak{c}$ and of norm smaller then $n$, which is $h_{\mathfrak{c}} j(\mathcal{R}, n)$. Hence by theorem 4.5 the abscissa of convergence is $\le 1$. ∎

**Remark 4.10** For every $s$ such that $L_{\mathfrak{c}}(\chi, s)$ converges we have the following identity, due to the multiplicativity of $\chi$ and the well-known formula for geometric series:

$$L_{\mathfrak{c}}(\chi, s) = \sum_{(\mathfrak{a},\mathfrak{c})=1} \frac{\chi(\mathfrak{a})}{\mathbf{N}\mathfrak{a}^s} = \prod_{\mathfrak{p}\nmid\mathfrak{c}} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{\mathbf{N}\mathfrak{p}^s}}.$$

The following is lemma Fried and Jarden [4, 5.5.19]:

**Theorem 4.11** *The function $L_{\mathfrak{c}}(\chi, s)$ has analytic continuation to the half-plane* $\mathrm{Re}(s) > 1 - 1/N$, *where $N$ is the degree of the number field $K$ of which $L_{\mathfrak{c}}$ is the $L_{\mathfrak{c}}$-series. If $\chi = 1$, then it has a simple pole at $s = 1$ with residue*

$$h_{\mathfrak{c}}\rho_{\mathfrak{c}} = \frac{h_{\mathfrak{c}} 2^{r_1} (2\pi)^{r_2} R_{\mathfrak{c}}}{w_{\mathfrak{c}}\sqrt{|\Delta_K|\mathbf{N}\mathfrak{c}}}.$$

Proof We have

$$\begin{aligned}
A_n &= \sum_{\mathcal{R}\in I(\mathfrak{c})/P_\mathfrak{c}} \sum_{\substack{\mathfrak{a}\in\mathcal{R}\\ \mathbf{N}\mathfrak{a}\le n}} \chi(\mathfrak{a}) \\
&= \sum_{\mathcal{R}\in I(\mathfrak{c})/P_\mathfrak{c}} \chi(\mathcal{R})(\rho_\mathfrak{c} n + O(n^{1-1/N}) \\
&= \sum_{\mathcal{R}\in I(\mathfrak{c})/P_\mathfrak{c}} \chi(\mathcal{R})\mathbf{1}(\mathcal{R}^{-1})(\rho_\mathfrak{c} n + O(n^{1-1/N}) \\
&\overset{3.20}{=} \langle \chi, \mathbf{1}\rangle_{I(\mathfrak{c})/P_\mathfrak{c}}(\rho_\mathfrak{c} n + O(n^{1-1/N})) \\
&\overset{3.23,\ 3.24}{=} \begin{cases} h_\mathfrak{c}\rho_\mathfrak{c} n + O(n^{1-1/N}) & \text{if } \chi = \mathbf{1}, \\ O(n^{1-1/N}) & \text{if } \chi \neq \mathbf{1}. \end{cases}
\end{aligned}$$

Hence by theorem 4.7, $L_\mathfrak{c}(s,\chi)$ has an analytic continuation to $\mathrm{Re}(s) > 1-1/N$. If $\chi = 1$, it has a simple pole with residue

$$h_\mathfrak{c}\rho_\mathfrak{c} = \frac{h_\mathfrak{c} 2^{r_1}(2\pi)^{r_2} R_\mathfrak{c}}{w_\mathfrak{c}\sqrt{|\Delta_K|}\mathbf{N}\mathfrak{c}}.$$

If $\chi \neq \mathbf{1}$ apply theorem 4.7 with $\rho = 0$ to conclude that $L_\mathfrak{c}(\chi, s)$ is analytic on the half-plane. ■

## 4.2 Artin $L$-functions

Most of the material in this section is from Dokchitser [3]. Representations are over $\mathbf{C}$. We will introduce Artin L-functions, and also cover some representation theory of Galois groups which will allow us to develop the Artin Formalism for Artin L-functions.

Throughout, we have the following:

- $F/K$ is a Galois extension of number fields.
- $\mathfrak{p}$ is a prime of $K$, $\mathfrak{q}$ lies above $\mathfrak{p}$.
- $D = D_{\mathfrak{q}/\mathfrak{p}}$, $I = I_{\mathfrak{q}/\mathfrak{p}}$, $\mathrm{Frob} = \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in D/I$, $G = \mathrm{Gal}(F/K)$.

If $V$ is a representation of $D$, write $V^I$ for the subspace of $I$-invariant vectors. As $I \triangleleft D$ this is a subrepresentation (if $v \in V^I$ then for $g \in G$ and $h \in I$ we have $hgv = gh'v = gv$ $(h' \in I)$).

**Definition 4.12** Let $I \subset D$ be finite groups (think: inertia respectively decomposition group), $\rho$ a $D$-representation. Then $\rho^I$ are the $I$-invariant vectors of $\rho$:

$$\rho^I = \{v \in \rho : g(v) = v \text{ for all } g \in I\}.$$

**Proposition 4.13** *If $I \triangleleft D$ (as in the case inertia group $\triangleleft$ decomposition group) then $\rho^I$ is a subrepresentation.*

Proof Easy verification. ■

**Definition 4.14** If $\lambda_i \in \mathbf{C}$, $g_i \in D$, write

$$\mathrm{Det}(\sum_i \lambda_i g_i | \rho) = \mathrm{Det}(\sum_i \lambda_i \rho(g_i))$$

**Example 4.15** The characteristic polynomial of $g \in D$ on $\rho$ with variable $T$ is $\mathrm{Det}(T - g|\rho)$.

**Definition 4.16** Let $F/K$ be a Galois extenion of number fields. Let

$$\rho\colon \mathrm{Gal}(F/K) \to \mathrm{Aut}_{\mathbf{C}}(\mathbf{C}^n)$$

be a representation. Let $\mathfrak{p}$ be a prime of $K$, $\mathfrak{q}|\mathfrak{p}$ be a prime of $F$ above $\mathfrak{p}$. Choose an element $\mathrm{Frob}_\mathfrak{p} \in D_{\mathfrak{q}/\mathfrak{p}}$ that maps to $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in D_{\mathfrak{q}/\mathfrak{p}}/I_{\mathfrak{q}/\mathfrak{p}}$. Then the **local polynomial of $\rho$ at $\mathfrak{p}$** is (we will show that this is independent of the choices made):

$$\begin{aligned} P_\mathfrak{p}(F/K, \rho, T) &= P_\mathfrak{p}(\rho, T) \\ &= \mathrm{Det}(1 - \mathrm{Frob}_\mathfrak{p} T | \rho^{I_\mathfrak{p}}), \end{aligned}$$

where $I_\mathfrak{p} = I_{\mathfrak{q}/\mathfrak{p}}$.

**Remark 4.17** This is essentially the characteristic polynomial $\Phi_{\mathfrak{q}/\mathfrak{p}}(\rho, T)$ of $\mathrm{Frob}_\mathfrak{p}$ on $\rho$. If

$$P_\mathfrak{p}(\rho, T) = 1 + a_1 T + \cdots + a_{n-1}T^{n-1} + a_n T^n$$

then

$$\Phi_{\mathfrak{q}/\mathfrak{p}}(\rho, T) = T^n + a_1 T^{n-1} + \cdots + a_{n-1} T + a_n.$$

**Remark 4.18** If $\dim \rho = 1$ then

$$P_\mathfrak{p}(\rho, T) = \begin{cases} 1 - \rho(\mathrm{Frob}_\mathfrak{p})T & \text{if } \rho^I = \rho, \\ 1 & \text{if } \rho^I = 0. \end{cases}$$

**Lemma 4.19** *$P_\mathfrak{p}(\rho, T)$ is independent of the choice of $\mathfrak{q}|\mathfrak{p}$ and of the choice of $\mathrm{Frob}_\mathfrak{p}$.*

Proof For fixed $\mathfrak{q}$, the independence is clear: two choices of $\mathrm{Frob}_\mathfrak{p}$ differ by an $i \in I$, which acts trivially on $\rho^I$. If $\mathfrak{q}'$ is a different prime over $\mathfrak{p}$, write $\mathfrak{q}' = g(\mathfrak{q})$ with $g \in \mathrm{Gal}(F/K)$ and observe that $\mathrm{Frob}'_\mathfrak{p} = g\,\mathrm{Frob}_\mathfrak{p}\, g^{-1}$ is a lift the Frobenius for $\mathfrak{q}'$. This shows that if $\lambda$ is an eigenvalue of $\mathrm{Frob}_\mathfrak{p}$ with eigenvector $v \in \rho^I$ then $\lambda$ is also an eigenvalue of $\mathrm{Frob}'_\mathfrak{p}$ with eigenvector $gv$. The converse reasining also works, hence we see that the eigenvalues with multiplicity of $\mathrm{Frob}_\mathfrak{p}$ and $\mathrm{Frob}'_\mathfrak{p}$ coincide, hence that their characteristic polynomials agree, hence that $P_\mathfrak{p}(\rho, T)$ is independent of the choice of $\mathfrak{q}$. ■

**Definition 4.20** Let $F/K$ be a Galois extension of number fields an $\rho$ a representation of $\mathrm{Gal}(F/K)$, $\mathfrak{c}$ a cycle of $K$. The **Artin $L_{\mathfrak{c}}$-function** of $\rho$ is defined by the Euler product

$$L_{\mathfrak{c}}(F/K,\rho,s) = L_{\mathfrak{c}}(\rho,s) = \prod_{\substack{\mathfrak{p}\nmid\mathfrak{c} \text{ prime}\\ \text{of } K}} \frac{1}{P_{\mathfrak{p}}(\rho,\mathbf{N}(\mathfrak{p})^{-s})}.$$

The polynomial $P_{\mathfrak{p}}(\rho,T)$ has the form (see remark 4.18) $1-(aT+bT^2+\cdots)$ hence we can write (ignoring convergence):

$$\begin{aligned}\frac{1}{P_{\mathfrak{p}}(\rho,T)} &= 1+(aT+bT^2+\cdots)+(aT+bT^2+\cdots)^2+\cdots\\ &= 1+a_{\mathfrak{p}}T+a_{\mathfrak{p}^2}T^2+\cdots\end{aligned}$$

Formally substituting this into the Euler product gives the expression (**Artin $L_{\mathfrak{c}}$-series**):

$$\begin{aligned}L_{\mathfrak{c}}(\rho,s) &= \prod_{\mathfrak{p}\nmid\mathfrak{c}}(1+a_{\mathfrak{p}}\mathbf{N}(\mathfrak{p})^{-s}+a_{\mathfrak{p}^2}\mathbf{N}(\mathfrak{p})^{-2s}+\cdots)\\ &= \sum_{(\mathfrak{a},\mathfrak{c})=1} a_{\mathfrak{a}}\mathbf{N}(\mathfrak{a})^{-s}\end{aligned}$$

where if $\mathfrak{a}$ decomposes as $\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$ we have $a_{\mathfrak{a}} = a_{\mathfrak{p}^{e_1}}\cdots a_{\mathfrak{p}^{e_r}}$. Note that grouping the ideals with equal norm yields an expression for $L_{\mathfrak{c}}(\rho,s)$ as an ordinary Dirichlet series.

**Lemma 4.21** *The $L_{\mathfrak{c}}$-series expression for $L_{\mathfrak{c}}(\rho,s)$ agrees with the Euler product on* $\mathrm{Re}(s)>1$, *where they converge absolutely to an analytic function.*

Proof It suffices to show that

$$\prod_{\mathfrak{p}\nmid\mathfrak{c}}(1+a_{\mathfrak{p}}\mathbf{N}(\mathfrak{p})^{-s}+a_{\mathfrak{p}^2}\mathbf{N}(\mathfrak{p})^{-2s}+\cdots)$$

converges absolutely on $\mathrm{Re}(s)>1$. This justifies rearrangement of terms and the Dirichlet series expression then proves analyticity.

$P_{\mathfrak{p}}(\rho,T)$ factorizes over $\mathbf{C}$ as

$$P_{\mathfrak{p}}(\rho,T) = (1-\lambda_1T)(1-\lambda_2T)\cdots(1-\lambda_kT)$$

for some $k\le\dim\rho$, $|\lambda_i|=1$. Hence the coefficients of

$$\begin{aligned}\frac{1}{P_{\mathfrak{p}}(\rho,T)} &= \frac{1}{\prod_i(1-\lambda_iT)}\\ &= \prod_i(1+\lambda_iT+\lambda_i^2T+\cdots)\\ &= 1+a_{\mathfrak{p}}T+a_{\mathfrak{p}^2}T+\cdots\end{aligned}$$

are bounded by those of

$$\frac{1}{(1-T)^{\dim\rho}} = (1+T+T^2+\cdots)^{\dim\rho}.$$

Hence

$$\begin{aligned}\prod_{\mathfrak{p}\nmid\mathfrak{c}}\sum_n |a_{\mathfrak{p}^n}||\mathbf{N}\mathfrak{p}^{-ns}| &\le \prod_{\mathfrak{p}\nmid\mathfrak{c}} \frac{1}{(1-|\mathbf{N}\mathfrak{p}^{-s}|)^{\dim\rho}} \\ &\le \prod_{p\text{ rational prime}} \left(\frac{1}{1-|p^{-s}|}\right)^{\dim\rho\cdot[K:\mathbf{Q}]} \\ &= \zeta(\sigma)^{\dim\rho\cdot[K:\mathbf{Q}]} \\ &< \infty\end{aligned}$$

where $\zeta$ is the Riemann $\zeta$-function of $\mathbf{Q}$ and $\sigma = \mathrm{Re}(s)$. ■

**Lemma 4.22**

*(i) Primes of $K$ are in bijection with* $\mathrm{Gal}(F/K)$*-orbits of primes of $F$ via*

$$\mathfrak{p} \leftrightarrow \textit{primes of } F \textit{ above } \mathfrak{p},$$

*i.e.* $\mathrm{Gal}(F/K)$ *acts transitively on these primes.*

*(ii) If $\mathfrak{q}$ is a prime of $F$ above $\mathfrak{p}$, then*

$$gD_{\mathfrak{q}} \mapsto g(\mathfrak{q})$$

*is a* $\mathrm{Gal}(F/K)$*-set isomorphism from $G/D_{\mathfrak{q}}$ to $\{$primes above $\mathfrak{p}\}$.*

*(iii)* $D_{g(\mathfrak{q})} = gD_{\mathfrak{q}}g^{-1}$, $I_{g(\mathfrak{q})} = gI_{\mathfrak{q}}g^{-1}$, $\mathrm{Frob}_{g(\mathfrak{q})/\mathfrak{p}} = g\,\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\,g^{-1}$.

Proof (i) follows directly from the transititity of the action. (ii) and (iii) are elementary to check. ■

**Corollary 4.23** *Let $F/L/K$ be an intermediate field. Let $H = \mathrm{Gal}(F/L$, $G = \mathrm{Gal}(F/K)$, $\mathfrak{q}$ a prime of $F$ over $\mathfrak{p}$. Then we have bijections*

$$\begin{aligned}\{\textit{primes of } L \textit{ above } \mathfrak{p}\} &\leftrightarrow \{\mathrm{Gal}(F/L)\textit{-orbits of primes of } F \textit{ above } \mathfrak{p}\} \\ &\leftrightarrow \{\textit{double cosets } HgD_{\mathfrak{q}}\}\end{aligned}$$

Proof The bijection between the first and second set is clear.

A bijection between the first and third set is the following. Map $\mathfrak{s}$ (a prime of $L$ above $\mathfrak{p}$) to the set of elements of $G$ that map $\mathfrak{q}$ to some prime above $\mathfrak{s}$, $X_{\mathfrak{s}}$ say. If $g \in X_{\mathfrak{s}}$ then the entire double coset $HgD_{\mathfrak{q}}$ is contained in $X_{\mathfrak{s}}$. Suppose $g, g' \in X_{\mathfrak{s}}$. Then $g(\mathfrak{q})|\mathfrak{s}, g'(\mathfrak{q})|\mathfrak{s}$, hence there is an $h \in H$ such that $hg(\mathfrak{q}) = g'(\mathfrak{q})$. This implies that $g'^{-1}hg \in D_{\mathfrak{q}}$, hence that $g \in HgD_{\mathfrak{q}}$. Hence every $X_{\mathfrak{s}}$ is equal to precisely one double coset $HgD_{\mathfrak{q}}$. ■

**Lemma 4.24** *If $V$ is an irreducible representation of $D$, then either*

- $V^I = 0$.
- *$V$ is 1-dimensional, lifted from $D/I$ (i.e. $D \to D/I \to \mathbf{C}^*$) (these kill $I$ and are determined by the action of* Frob*).*

Proof $V^I$ is a subrepresentation, hence $V^I = 0$ or $V^I = V$. If $V^I = V$ then the action of $D$ factors through $D/I$. The latter is abelian hence $V$ is 1-dimensional. ■

**Remark 4.25** So representations of $D$ look like $V = A \oplus B$ with $A^I = 0$ and $B = V^I = \bigoplus$ 1-d reps of $D/I$.

**Notation 4.26** Let $(V, \rho)$ be a representation of $D$.

$$\begin{aligned}\Phi_{\mathfrak{q}/\mathfrak{p}}(V,t) &= \mathrm{Det}_{V^I}(t\cdot \mathrm{Id} - \rho(\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}))\\ &= \text{characteristic polynomial of Frob on } V^I.\end{aligned}$$

**Lemma 4.27** *Let $\psi\colon D \to D/I \to \mathbf{C}^*$ be a 1-dimensional representation of $D$ with $\psi(\mathrm{Frob}) = \zeta$. Then*

$$\begin{aligned}\langle \psi, V\rangle &= \langle \psi, V^I\rangle\\ &= \textit{multiplicity of } (t-\zeta) \textit{ in } \Phi_{\mathfrak{q}/\mathfrak{p}}(V,t).\end{aligned}$$

Proof We have

$$\begin{aligned}\langle \psi, V\rangle &= \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}[D]}(\mathbf{C}, V)\\ &= \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}[D]}(\mathbf{C}, V^I)\\ &= \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}[D]}(\mathbf{C}, \bigoplus \text{1-d reps of } D/I).\end{aligned}$$

$1 \in \mathbf{C}$ can be send to a 1-dimensional summand if and only if Frob acts as multiplication by $\zeta$ on that summand, hence

$$\dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}[D]}(\mathbf{C}, \bigoplus \text{1-d reps of } D/I) = \text{multiplicity of } (t-\zeta) \text{ in } \Phi_{\mathfrak{q}/\mathfrak{p}}(V,t).$$

■

**Remark 4.28** Hence $\Phi(V,t)$ encodes the multiplicities of the 1-dimensional representations of $D/I$ in $V$.

If $G$ is a group $(V, \rho)$ a representation and $x \in G$ denote by $V^x$ the representation of $G$ which is $V$ "after conjugating by $x$":

$$\rho^x(g) = \rho(x^{-1}gx).$$

**Proposition 4.29** *Let $F/L/K$ be an intermediate field, $(V, \rho)$ a representation of $\operatorname{Gal}(F/L)$ with character $\chi_\rho$. Then*

$$\Phi_{\mathfrak{q}/\mathfrak{p}}(\operatorname{Res}_D \operatorname{Ind}_H^G V, t) = \prod_{\mathfrak{s}} \Phi_{\mathfrak{q}_i/\mathfrak{s}} \left( \operatorname{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V, t^{f_{\mathfrak{s}/\mathfrak{p}}} \right)$$

*where $\mathfrak{s}$ runs over the primes of $L$ above $\mathfrak{p}$ and $\mathfrak{q}_i$ lies above $\mathfrak{s}$.*

Proof We will show that the left hand side and the right hand side have the same roots, with the same multiplicities. Note that the roots are $f_{\mathfrak{q}/\mathfrak{p}}$-th roots of unity. Let $\zeta$ be such a root and take

$$\psi \colon D \to D/I \to \mathbf{C}^*$$

with $\psi(\text{Frob}) = \zeta$.

Then by remark 4.28:

$$\text{multiplicity of } t - \zeta \text{ in LHS} = \langle \psi, \operatorname{Res}_D \operatorname{Ind}_H^G V \rangle_D.$$

Note that for $x \in G$ the character of $(W_x, \rho^x)$ (remember: first conjugating by $x$) is $\chi_\rho^x$ (also first conjugate by $x$ before applying $\chi_\rho$). Let $X$ be a system of representatives of $H \backslash G / D$. Then by Mackey's formula:

$$\langle \psi, \operatorname{Res}_D \operatorname{Ind}_H^G V \rangle_D = \sum_{x \in X} \langle \psi, \operatorname{Ind}^D_{x^{-1}Hx \cap D} \operatorname{Res}^{x^{-1}Hx}_{x^{-1}Hx \cap D} V_x \rangle_D.$$

Since $\psi$ is one dimensional, $\chi_\psi = \psi$. By lemma 3.52, we have

$$\sum_{x \in X} \langle \psi, \operatorname{Ind}^D_{x^{-1}Hx \cap D} \operatorname{Res}^{x^{-1}Hx}_{x^{-1}Hx \cap D} V_x \rangle_D = \sum_{x \in X} \langle \psi, \operatorname{Ind}^D_{x^{-1}Hx \cap D} \operatorname{Res}^{x^{-1}Hx}_{x^{-1}Hx \cap D} \rho^x \rangle_D. \tag{4.2}$$

The next step is rather involved. Let $g = \#G$ and $h = \#x^{-1}Hx \cap D$. Note that $h$ is also equal to $\#H \cap x^{-1}Dx$. We have by definition of the inner product, of

Ind and of Res:

$$
\begin{aligned}
&\sum_{x\in X}\langle \psi, \operatorname{Ind}^{D}_{x^{-1}Hx\cap D}\operatorname{Res}^{x^{-1}Hx}_{x^{-1}Hx\cap D}\rho^{x}\rangle_{D}\\
&=\sum_{d\in D}\psi(d)\frac{1}{h}\sum_{\substack{s\in D\\ s^{-1}ds\in x^{-1}Hx\cap D}}\chi_{\rho^{x}}(s^{-1}ds)^{*}\\
&=\sum_{d\in D}\psi(d)\frac{1}{h}\sum_{\substack{s\in x^{-1}Dx\\ (xsx^{-1})^{-1}d(xsx^{-1})\\ \in\\ x^{-1}Hx\cap D}}\chi_{\rho^{x}}((xsx^{-1})^{-1}d(xsx^{-1}))^{*}\\
&=\sum_{d\in D}\psi(d)\frac{1}{h}\sum_{\substack{s\in x^{-1}Dx\\ s^{-1}x^{-1}dxs\\ \in\\ H\cap x^{-1}Dx}}\chi_{\rho^{x}}((xsx^{-1})^{-1}d(xsx^{-1}))^{*}\\
&=\sum_{d\in D}\psi(d)\frac{1}{h}\sum_{\substack{s\in x^{-1}Dx\\ s^{-1}x^{-1}dxs\\ \in\\ H\cap x^{-1}Dx}}\chi_{\rho}((s^{-1}x^{-1}dxs))^{*}\\
&=\sum_{d\in x^{-1}Dx}\psi(xdx^{-1})\frac{1}{h}\sum_{\substack{s\in x^{-1}Dx\\ s^{-1}ds\in H\cap x^{-1}Dx}}\chi_{\rho}(s^{-1}ds).
\end{aligned}
$$

The bijection from corollary 4.23 gives a bijection between primes $\mathfrak{s}$ of $L$ over $\mathfrak{p}$ and double cosets $HgD$, mapping a coset represented by $x$ to $x(\mathfrak{q})$. Also note that $x^{-1}Dx = x^{-1}D_{\mathfrak{q}/\mathfrak{p}}x = D_{x^{-1}(\mathfrak{q})/\mathfrak{p}}$. Hence $H\cap x^{-1}Dx\cap H = D_{x^{-1}(\mathfrak{q})/\mathfrak{s}}$ where $\mathfrak{s}$ is the prime of $L$ over which $x^{-1}(\mathfrak{q})$ is lying. Denote $x^{-1}(\mathfrak{q}) = \mathfrak{q}_i$. We see that

$$
\begin{aligned}
&\sum_{d\in x^{-1}Dx}\psi(xdx^{-1})\frac{1}{h}\sum_{\substack{s\in x^{-1}Dx\\ s^{-1}ds\in H\cap x^{-1}Dx}}\chi_{\rho}(s^{-1}ds)\\
&=\langle \psi^{x^{-1}}, \operatorname{Ind}^{D_{\mathfrak{q}_i/\mathfrak{p}}}_{D_{\mathfrak{q}_i/\mathfrak{s}}}\operatorname{Res}^{H}_{D_{\mathfrak{q}_i/\mathfrak{s}}}\chi_{\rho}\rangle_{D_{\mathfrak{q}_i/\mathfrak{p}}}.
\end{aligned}
$$

Using this in eq. (4.2) we see that (in the second sum $\mathfrak{s}$ is the prime of $L$ over $\mathfrak{p}$ corresponding to the coset represented by $x^{-1}$ (i.e. $Hx^{-1}D$), and $\mathfrak{q}_i = x^{-1}\mathfrak{q}$):

$$
\begin{aligned}
&\sum_{x\in X}\langle \psi, \operatorname{Ind}^{D}_{x^{-1}Hx\cap D}\operatorname{Res}^{x^{-1}Hx}_{x^{-1}Hx\cap D}\rho^{x}\rangle_{D}\\
&=\sum_{\substack{\mathfrak{s}\mid\mathfrak{p}\\ \mathfrak{s}\text{ prime of }L}}\langle \psi^{x^{-1}}, \operatorname{Ind}^{D_{\mathfrak{q}_i/\mathfrak{p}}}_{D_{\mathfrak{q}_i/\mathfrak{s}}}\operatorname{Res}^{H}_{D_{\mathfrak{q}_i/\mathfrak{s}}}\chi_{\rho}\rangle_{D_{\mathfrak{q}_i/\mathfrak{p}}}.
\end{aligned}
$$

By Frobenius reciprocity:

$$\begin{aligned}
&\sum_{\substack{\mathfrak{s}|\mathfrak{p}\\ \mathfrak{s}\text{ prime of }L}} \langle \psi^{x^{-1}}, \operatorname{Ind}_{D_{\mathfrak{q}_i/\mathfrak{s}}}^{D_{\mathfrak{q}_i/\mathfrak{p}}} \operatorname{Res}^{H}_{D_{\mathfrak{q}_i/\mathfrak{s}}} \chi_\rho \rangle_{D_{\mathfrak{q}_i/\mathfrak{p}}}\\
&= \sum_{\substack{\mathfrak{s}|\mathfrak{p}\\ \mathfrak{s}\text{ prime of }L}} \langle \operatorname{Res}_{D_{\mathfrak{q}_i/\mathfrak{s}}}^{D_{\mathfrak{q}_i/\mathfrak{p}}} \psi^{x^{-1}}, \operatorname{Res}^{H}_{D_{\mathfrak{q}_i/\mathfrak{s}}} \chi_\rho \rangle_{D_{\mathfrak{q}_i/\mathfrak{s}}}
\end{aligned}$$

We have $\operatorname{Frob}_{\mathfrak{q}/\mathfrak{p}}^{f_{\mathfrak{s}/\mathfrak{p}}} = \operatorname{Frob}_{\mathfrak{q}/\mathfrak{s}}$. Hence $\psi(\operatorname{Frob}_{\mathfrak{q}/\mathfrak{s}}) = \zeta^{f_{\mathfrak{s}/\mathfrak{p}}}$, $\psi(\operatorname{Frob}_{\mathfrak{q}_i/\mathfrak{s}}) = \zeta^{f_{\mathfrak{s}/\mathfrak{p}}}$. Hence by applying 4.28 to $F/L$ we see that

$$\begin{aligned}
&\sum_{\substack{\mathfrak{s}|\mathfrak{p}\\ \mathfrak{s}\text{ prime of }L}} \langle \operatorname{Res}_{D_{\mathfrak{q}_i/\mathfrak{s}}}^{D_{\mathfrak{q}_i/\mathfrak{p}}} \psi^{x^{-1}}, \operatorname{Res}^{H}_{D_{\mathfrak{q}_i/\mathfrak{s}}} \chi_\rho \rangle_{D_{\mathfrak{q}_i/\mathfrak{s}}}\\
&= \sum_{\substack{\mathfrak{s}|\mathfrak{p}\\ \mathfrak{s}\text{ prime of }L}} \text{mult. of } (t - \zeta^{f_{\mathfrak{s}/\mathfrak{p}}}) \text{ in } \Phi_{\mathfrak{q}_i/\mathfrak{s}}(\operatorname{Res}^{H}_{D_{\mathfrak{q}_i/\mathfrak{s}}} V, t)\\
&= \sum_{\substack{\mathfrak{s}|\mathfrak{p}\\ \mathfrak{s}\text{ prime of }L}} \text{mult. of } (t - \zeta) \text{ in } \Phi_{\mathfrak{q}_i/\mathfrak{s}}(\operatorname{Res}^{H}_{D_{\mathfrak{q}_i/\mathfrak{s}}} V, t^{f_{\mathfrak{s}/\mathfrak{p}}}). \qquad \blacksquare
\end{aligned}$$

**Lemma 4.30** *Let $F/K$ be a Galois extension of number fields,*

$$G = \operatorname{Gal}(F/K),$$

*$N \lhd G$, $\mathfrak{q}$ above $\mathfrak{s}$ above $\mathfrak{p}$ primes of $F$ resp. $F^N$ resp. $K$. We have $\operatorname{Gal}(F^N/K) \cong G/N$. Let $\pi\colon G \to G/N$. Then:*

*(i)* $D_{\mathfrak{s}/\mathfrak{p}} = D_{\mathfrak{q}/\mathfrak{p}}N/N$,

*(ii)* $I_{\mathfrak{s}/\mathfrak{p}} = I_{\mathfrak{q}/\mathfrak{p}}N/N$,

*(iii) and if* $\operatorname{Frob}_{\mathfrak{p}} \in D_{\mathfrak{q}/\mathfrak{p}}$ *acts as the Frobenius automorphism on* $\mathcal{O}_F/\mathfrak{q}$ *then* $\pi(\operatorname{Frob}_{\mathfrak{p}}) \in D_{\mathfrak{s}/\mathfrak{p}}$ *is a Frobenius element for* $\mathfrak{s}/\mathfrak{p}$.

Proof (i) $D_{\mathfrak{q}/\mathfrak{p}}$ and $N$ both preserve $\mathfrak{s}$, hence $D_{\mathfrak{s}/\mathfrak{p}} \supset D_{\mathfrak{q}/\mathfrak{p}}N$. But also

$$\begin{aligned}
\#D_{\mathfrak{s}/\mathfrak{q}} &= e_{\mathfrak{s}/\mathfrak{p}} f_{\mathfrak{s}/\mathfrak{p}}\\
&= \frac{e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}}}{e_{\mathfrak{q}/\mathfrak{s}} f_{\mathfrak{q}/\mathfrak{s}}}\\
&= \frac{\#D_{\mathfrak{q}/\mathfrak{p}}}{\#D_{\mathfrak{q}/\mathfrak{s}}}\\
&= \frac{\#D_{\mathfrak{q}/\mathfrak{p}}}{\#D_{\mathfrak{q}/\mathfrak{p}} \cap N}\\
&= \frac{\#D_{\mathfrak{q}/\mathfrak{p}}N}{\#N}.
\end{aligned}$$

(ii) Smiliar with $e$ instead of $ef$.

(iii) $\mathcal{O}_{F^N}/\mathfrak{s}$ is a subfield of $\mathcal{O}_F/\mathfrak{q}$ and both fields are over $\mathcal{O}_K/\mathfrak{p}$. The Frobenius raises elements to the $\mathbf{N}\mathfrak{p}$-th power, and is characterized by this. ∎

**Proposition 4.31**

*Let $F/K$ be a Galois extension of number fields, $\rho$ a $\mathrm{Gal}(F/K)$-representation.*

*(i) If $\rho'$ is another $\mathrm{Gal}(F/K)$-representation, then*

$$L_\mathfrak{c}(\rho \oplus \rho', s) = L_\mathfrak{c}(\rho, s)L_\mathfrak{c}(\rho', s)$$

*(ii) If $N \triangleleft \mathrm{Gal}(F/K)$ lies in $\ker\rho$, or, equivalently, if $\rho$ factors as $\rho'' \circ \pi$ in*

$$\mathrm{Gal}(F/K) \xrightarrow{\pi} \mathrm{Gal}(F/K)/N \cong \mathrm{Gal}(F^N/K) \xrightarrow{\rho''} \mathrm{Aut}_\mathbf{C}(\mathbf{C}^n)$$

*then*

$$L_\mathfrak{c}(F/K, \rho, s) = L_\mathfrak{c}(F^N/K, \rho'', s).$$

*(iii) (Artin Formalism) If $\rho = \mathrm{Ind}_H^{\mathrm{Gal}(F/K)} \rho'''$ for a representation $\rho'''$ of $H < \mathrm{Gal}(F/K)$ then*

$$L_\mathfrak{c}(F/K, \rho, s) = L_\mathfrak{c}(F/F^H, \rho''', s).$$

*(even though $\mathfrak{c}$ is not a cycle of $F^H$ but of $K$ we make sense of this by simply summing over those ideals of $F^H$ that are relatively prime to $\mathfrak{c}$ (this still makes sense)).*

Proof It suffices to check each statement prime-by-prime for the local polynomials.

(i) We have

$$\begin{aligned} P_\mathfrak{p}(\rho \oplus \rho', T) &= \det(1 - \mathrm{Frob}_\mathfrak{p} T | (\rho \oplus \rho')^{I_\mathfrak{p}}) \\ &= \det(1 - \mathrm{Frob}_\mathfrak{p} T | \rho^{I_\mathfrak{p}} \oplus \rho'^{I_\mathfrak{p}}) \\ &= \det(1 - \mathrm{Frob}_\mathfrak{p} T | \rho^{I_\mathfrak{p}}) \det(1 - \mathrm{Frob}_\mathfrak{p} T | \rho'^{I_\mathfrak{p}}) \\ &= P_\mathfrak{p}(\rho, T) P_\mathfrak{p}(\rho', T). \end{aligned}$$

(ii) Apply lemma 4.30:

$$\begin{aligned} P_\mathfrak{p}(\rho, T) &= \det(1 - \mathrm{Frob}_\mathfrak{p} T | \rho^{I_{\mathfrak{q}/\mathfrak{p}}}) \\ &= \det(1 - \rho(\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}})T | \rho^{I_{\mathfrak{q}/\mathfrak{p}}}) \\ &= \det(1 - \rho(\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}})T | \rho^{I_{\mathfrak{q}/\mathfrak{p}}N/N}) \\ &= \det(1 - \rho''(\pi(\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}))T | \rho^{I_{\mathfrak{q}/\mathfrak{p}}N/N}) \\ &= \det(1 - \rho''(\mathrm{Frob}_{\mathfrak{s}/\mathfrak{p}})T | \rho^{I_{\mathfrak{s}/\mathfrak{p}}}) \\ &= L(F^N/K, \rho'', s). \end{aligned}$$

(iii) This follows from Artin's Induction Theorem and the fact that the local polynomials are essentially the characteristic polynomials of Frobeniusses. Note that on the one hand we have ($\mathfrak{p}$ denotes primes of $K$, $\mathfrak{s}$ denotes primes of $F^H$, $\mathfrak{q}$ denotes primes of $F$):

$$L_{\mathfrak{c}}(F/K, \rho, s) = \prod_{\mathfrak{p}\nmid\mathfrak{c}} \frac{1}{P_{\mathfrak{p}}(\rho, s)}.$$

On the other hand we have

$$\begin{aligned} L_{\mathfrak{c}}(F/F^H, \rho''', s) &= \prod_{\mathfrak{s}\nmid\mathfrak{c}} \frac{1}{P_{\mathfrak{s}}(\rho''', s)} \\ &= \prod_{\mathfrak{p}\nmid\mathfrak{c}} \prod_{\mathfrak{s}|\mathfrak{p}} \frac{1}{\det(1 - \mathrm{Frob}_{\mathfrak{s}/\mathfrak{p}} \, \mathbf{N}\mathfrak{s}^{-s}} \\ &= \prod_{\mathfrak{p}\nmid\mathfrak{c}} \prod_{\mathfrak{s}|\mathfrak{p}} \frac{1}{\det(1 - \mathrm{Frob}_{\mathfrak{s}/\mathfrak{p}} \, \mathbf{N}\mathfrak{p}^{-f_{\mathfrak{s}/\mathfrak{p}} s}}. \end{aligned}$$

Hence we are done if we can show that

$$P_{\mathfrak{p}}(\rho, T) = \prod_{\mathfrak{s}|\mathfrak{p}} P_{\mathfrak{s}}(\rho''', T^{f_{\mathfrak{s}/\mathfrak{p}}}).$$

The local polynomial $P_{\mathfrak{p}}$ corresponds to the characteristic function $\Phi_{\mathfrak{q}/\mathfrak{p}}$ by reversing the coefficients: the highest coefficient becomes the lowest and vice versa. If $f = a_0 + a_1 T + \cdots + a_n T^n$ then call $f_{\mathrm{rev}} = a_n + a_{n-1} T + \cdots + a_0 T^n$. We then have $P_{\mathfrak{p},\mathrm{rev}} = \Phi_{\mathfrak{q}/\mathfrak{p}}$. Note that rev commutes with multiplication of polynomials: if $f = \sum_{i=0}^n a_i X^i$ and $g = \sum_{j=0}^m b_j X^j$ then both $(fg)_{\mathrm{rev}}$ and $f_{\mathrm{rev}} g_{\mathrm{rev}}$ are equal to

$$\sum_{k=0}^{m+n} \sum_{\substack{u+v= \\ m+n-k}} a_u b_v X^k.$$

Applying rev we see that what we want is equivalent to

$$\Phi_{\mathfrak{q}/\mathfrak{p}}(\mathrm{Res}_{D_{\mathfrak{q}/\mathfrak{p}}} \rho, T) = \prod_{\mathfrak{s}} \Phi_{\mathfrak{q}_i/\mathfrak{s}}(\mathrm{Res}_{D_{\mathfrak{q}_i/\mathfrak{s}}} \rho''', T^{f_{\mathfrak{s}/\mathfrak{q}}}),$$

which is proposition 4.29. ∎

**Theorem 4.32** *Let $F/K$ be a Galois extension of number fields and $\rho$ a 1-dimensional* Gal$(F/K)$*-representation. Then*

*(i)* *$L(F/K, \rho, s)$ has an analytic continuation to* $\mathrm{Re}(s) > 1 - 1/[K : \mathbf{Q}]$, *except for a simple pole at $s = 1$ if $\rho = \mathbf{1}$.*

*(ii)* *If $\rho \neq \mathbf{1}$ then $L(\rho, 1) \neq 0$.*

Proof Note that $\ker\rho \lhd \mathrm{Gal}(F/K)$. Apply proposition 4.31 (ii) to see that

$$L_{\mathfrak{c}}(F/K, \rho, s) = L_{\mathfrak{c}}(F^{\ker\rho}/K, \rho'', s)$$

where $\rho'' = \rho \circ \pi$ as in proposition 4.31 (ii). In particular, $\rho''$ is one-dimensional. Hence we can assume without loss of generality that $F = F^{\ker\rho}$. But note that

$$\begin{aligned} F = F^{\ker\rho} &\iff \ker\rho = \{1\} \lhd \mathrm{Gal}(F/K) \quad \text{(Galois correspondence)} \\ &\iff \rho\colon\ \mathrm{Gal}(F/K) \to \mathbf{C}^* \text{ is an injective group homomorphism} \\ &\implies \mathrm{Gal}(F/K) \text{ is abelian} \end{aligned}$$

(i) Is exactly the statement of theorem 4.38, since $\rho$ is a one-dimensional representation, that is, a character.

(ii) This follows from proposition 4.31: first apply (iii) and then (i). If $G$ is a group denote by $\mathrm{reg}_G$ its regular representation. Then $\{1\} < G$, $\mathbf{C}e_1$ is invariant under $\{1\}$ and

$$\mathbf{C}^{\#G} \cong \bigoplus_{g \in G/\{1\}} g\mathbf{C}e_1.$$

Hence $\mathrm{Ind}_{\{1\}}^G \mathbf{1} = \mathrm{reg}_G$.

By theorem 3.39 the irreducible representations of $G$ are all one-dimensional (that is, characters). By corollary 3.30 we have

$$\mathrm{reg}_G = \sum_{\substack{\chi \text{ irred.} \\ \text{char. of G}}} \chi.$$

Hence we get

$$\begin{aligned} \zeta_F(s) &= L(F/F, \mathbf{1}, s) \\ &= L(F/F^{\{\mathrm{Id}\}}, \mathbf{1}, s) \\ &= L(F/K, \mathrm{Ind}_{\{\mathrm{Id}\}}^G \mathbf{1}, s) \\ &= L(F/K, \mathrm{reg}_G, s) \\ &= L(F/K, \sum_{\substack{\chi \text{ irred.} \\ \text{char. of G}}} \chi, s) \\ &= \prod_{\substack{\chi \text{ irred.} \\ \text{char. of G}}} L(F/K, \chi, s) \quad \text{(proposition 4.31 (i))} \\ &= \zeta_K(s) \prod_{\substack{\chi \neq \mathbf{1} \text{ irred.} \\ \text{char. of G}}} L(F/K, \chi, s). \end{aligned}$$

As both $\zeta$-functions ahve a simple pole at 1 and each $L(F/K, \chi, s)$ is analytic at $s = 1$, it follows that no $L(F/K, \chi, s)$ can have a zero at $s = 1$, for else it would cancel the pole of $\zeta_K(s)$ there. ■

**Proposition 4.33** *Let $F/K$ be a Galois extension of number fields and $\rho$ a $\mathrm{Gal}(F/K)$-representation.*

*(i) For some $n \geq 1$, $L(\rho^{\oplus n}, s)$ has a meromorphic continuation to $1 - 1/[K : \mathbf{Q}]$. If $\langle \rho, \mathbf{1} \rangle = 0$ it is analytic and non-zero at $s = 1$.*

*(ii) If $\rho \neq \mathbf{1}$ is irreducible, then $L(\rho, s)$ has an analytic continuation to $s = 1$, where the function does not vanish.*

Proof (i) Write

$$\rho^{\oplus n} \oplus \bigoplus_i \mathrm{Ind}_{H_i}^G \psi_i \cong \bigoplus_j \mathrm{Ind}_{H'_j}^G \psi'$$

where $G = \mathrm{Gal}(F/K)$, as in Artin's Induction Theorem. By proposition 4.31 we have on $\mathrm{Re}(s) > 1$

$$L(\rho, s)^n = \frac{\prod_j L(F/K, \mathrm{Ind}\,\psi'_j, s)}{\prod_i L(F/K, \mathrm{Ind}\,\psi_i, s)} = \frac{\prod_j L(F/F^{H'_j}, \psi'_j, s)}{\prod_i L(F/F^{H_i}, \psi_i, s)}.$$

By theorem 4.32 the right hand side has a meromorphic continuation to $\mathrm{Re}(s) > 1 - 1/[K : \mathbf{Q}]$. If $\langle \rho, \mathbf{1} \rangle = 0$ the $\psi_i, \psi'_j$ can be taken to be non-trivial, in which case the right hand side is also analytic and non-zero at $s = 1$.

(ii) $L(\rho, s)^n$ is analytic and non-zero at $s = 1$ for some $n$. On $\mathrm{Re}(s) > 1$, $L(\rho, s)$ is an analytic branch of the $n$-th root of $L(\rho, s)^n$, and hence as an analytic continuation to $s = 1$. ■

## 4.3 The Artin Reciprocity Law

Later we will see in theorem 4.38 that $L$-series of characters of Galois groups (also defined in theorem 4.38) admit an analytic continuation. We showed this for $L$-series of characters of the ideal class group in theorem 4.11. We can use this last result to prove the first, using the relation between these two groups provided by Artin's Reciprocity Law from Class Field Theory. This law will be stated here, but not proven.

**Definition 4.34** Let $K/k$ be Galois, $\mathfrak{c}$ a cycle of $k$ divisible by all ramified primes of $k$. Set

$$\mathcal{N}(\mathfrak{c}) = \{N_k^K(\mathfrak{a}) | \mathfrak{a} \in I_K, (\mathfrak{a}, \mathfrak{c}) = 1\}.$$

Note that $\mathcal{N}(\mathfrak{c}) \subset I(\mathfrak{c})$ as none of the prime ideals of $\mathfrak{a}$ lie above any of the ideals in $\mathfrak{c}$, hence $(N_k^K(\mathfrak{a}), \mathfrak{c}) = 1$, hence $N_k^K(\mathfrak{a}) \in I(\mathfrak{c})$.

**Definition 4.35** Let $K/k$ be an abelian extension of number fields. Let $\mathfrak{c}$ be a cycle of $k$ divisible by the ramifying primes of $k$. The group homomorphism

$$\begin{aligned} \omega \colon I(\mathfrak{c}) &\to \mathrm{Gal}(K/k) \\ \mathfrak{p} &\mapsto \mathrm{Frob}_{\mathfrak{p}} \end{aligned}$$

defined on prime ideals and extended multiplicatively is called the **reciprocity law map**, or the **Artin map**. It is well defined since all $\mathfrak{p} \in I(\mathfrak{c})$ are unramified and since $\mathrm{Gal}(K/k)$ is abelian.

**Theorem 4.36** *For every cycle $\mathfrak{c}$ divisible by the ramifying primes, the reciprocity map*

$$\omega \colon I(\mathfrak{c}) \to \mathrm{Gal}(K/k)$$

*is surjective.*

Proof This requires the global norm index inequality, which will not be treated in this thesis. We refer to Lang [9, XV.§1]. ∎

**Theorem 4.37 (Artin Reciprocity Law)** *There exists a cycle $\mathfrak{c}$ such that $P_{\mathfrak{c}}$ is contained in the kernel of the reciprocity map. Such a cycle will be called **admissable**. For such a cycle, the kernel of the reciprocity map is precisely $P_{\mathfrak{c}}\mathcal{N}(\mathfrak{c})$. Hence we get an isomorphism*

$$\omega \colon I(\mathfrak{c})/P_{\mathfrak{c}}\mathcal{N}(\mathfrak{c}) \to \mathrm{Gal}(K/k)$$

*from the Artin map. This is the Artin reciprocity law.*

Proof This is the fundamental theorem of class field theory, and we will not prove it here. We refer to Lang [9, X.§3]. ∎

**Theorem 4.38** *Let $F/K$ be a Galois extension of number fields with*

$$\mathrm{Gal}(F/K)$$

*abelian, and $\psi\colon \mathrm{Gal}(F/K) \to \mathbf{C}^*$ a homomorphism (hence a character). Then*

$$L_*(\psi, s) := \prod_{\substack{\mathfrak{p} \text{ prime of } K \\ \text{unram. in } K}} \frac{1}{1 - \psi(\mathrm{Frob}_{\mathfrak{p}})\mathbf{N}\mathfrak{p}^{-s}}$$

*has an analytic continuation to $\mathrm{Re}(s) > 1 - 1/[K : \mathbf{Q}]$, except for a simple pole at $s = 1$ when $\psi = 1$.*

Proof Let $\mathfrak{c}$ be an admissable cycle of $K/k$. Then

$$I(\mathfrak{c})/P_{\mathfrak{c}} \to I(\mathfrak{c})/P_{\mathfrak{c}}\mathcal{N}(\mathfrak{c}) \xrightarrow{\sim} \mathrm{Gal}(F/K) \xrightarrow{\mathrm{Frob}_{\mathfrak{p}}} \mathbf{C}^*$$

is a character $\chi$ on $I(\mathfrak{c})/P_{\mathfrak{c}}$, and composed with the map $I(\mathfrak{c}) \to I(\mathfrak{c})/P_{\mathfrak{c}}$ it gives $\mathfrak{p} \mapsto \psi(\mathrm{Frob}_{\mathfrak{p}})$. Hence we can apply theorem 4.11 to deduce that $L_{\mathfrak{c}}(\chi, s)$ has an analytic continuation to $\mathrm{Re}(s) > 1 - 1/[K : \mathbf{Q}]$ with only a simple pole at $s = 1$ if $\chi = 1$, that is if $\psi = 1$. Since $L_*(\psi, s)$ and $L_{\mathfrak{c}}(\chi, s)$ only differ in a finite number of factors, this does not alter analytic aspects. ∎

# Chapter 5

# Chebotarev's density theorem

We now give a proof of Chebotarev's Density Theorem.

**Theorem 5.1** *The equivalence $\sim$ denoting the property of differing by a function analytic at $s = 1$, we have:*

$$\log \frac{1}{s-1} \sim \sum_{\mathfrak{p}} \frac{1}{\mathbf{N}\mathfrak{p}^s}.$$

PROOF See Lang [9, theorem VIII.§3.6]. ■

**Definition 5.2** Let $M$ be a set primes of a number field $K$. The **Dirichlet density** of $M$ is the limit

$$\lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in M} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\log \frac{1}{s-1}}$$

if it exists. The $s \to 1^+$ means that the limit is taken for real $s > 1$. The **natural density** of $M$ is the limit

$$\lim_{n \to \infty} \frac{\#\{\mathfrak{p} \in M : \mathbf{N}\mathfrak{p} \leq n\}}{\#\{\mathfrak{p} \text{ prime of } K : \mathbf{N}\mathfrak{p} \leq n\}}$$

if it exists.

**Proposition 5.3** *If a set primes $M$ of a number field $K$ has a natural density $d$ then $M$ also has a Dirichlet density, and the Dirichlet density of $M$ is then also equal to $d$.*

PROOF Adapted from Descombes [2, chapter 8] where the case $K = \mathbf{Q}$ is proven, we do the general case. For an alternative proof see Goldstein [5, theorem 14-1-2].

Let $\Pi \subset I_K$ denote the subset of prime ideals of $K$.

Let $\vartheta$ and $\eta$ be the indicator functions of $M$ resp. $\Pi$. For $n \in \mathbf{N}$ define

$$\begin{aligned} \Theta(n) &= \sum_{\substack{\mathfrak{a}\in I_K\\ \mathbf{N}\mathfrak{a}\le n}} \vartheta(\mathfrak{a}),\\ H(n) &= \sum_{\substack{\mathfrak{a}\in I_K\\ \mathbf{N}\mathfrak{a}\le n}} \eta(\mathfrak{a}). \end{aligned} \qquad \blacksquare$$

Then

$$\frac{\Theta(n)}{H(n)} \xrightarrow{n\to\infty} d.$$

For real $\sigma$, $\zeta(\sigma) = \sum_{\mathfrak{a}\in I_K} \mathbf{N}\mathfrak{a}^{-\sigma}$ majorizes

$$\sum_{\mathfrak{a}\in I_K} \vartheta(\mathfrak{a})\frac{1}{\mathbf{N}\mathfrak{a}^{\sigma}} \quad \text{and} \quad \sum_{\mathfrak{a}\in I_K} \eta(\mathfrak{a})\frac{1}{\mathbf{N}\mathfrak{a}^{\sigma}},$$

hence these two sums are convergent for $\sigma > 1$. Denote their sums by $S(\sigma)$ resp. $T(\sigma)$.

We have

$$\begin{aligned} S(\sigma) &= \sum_{\mathfrak{a}} \vartheta(\mathfrak{a})\mathbf{N}\mathfrak{a}^{-\sigma} = \sum_{\mathfrak{p}\in\Pi} \mathbf{N}\mathfrak{p}^{-\sigma}\\ T(\sigma) &= \sum_{\mathfrak{a}} \eta(\mathfrak{a})\mathbf{N}\mathfrak{a}^{-\sigma} = \sum_{\mathfrak{p}\in\Pi} \mathbf{N}\mathfrak{p}^{-\sigma}. \end{aligned}$$

The limit we are interested in is equal to the limit of $S(\sigma)/T(\sigma)$ as $\sigma \to 1^+$ by theorem 5.1. Note that the number of ideals in $\Pi$ with norm precisely $k$ is $\Theta(k) - \Theta(k-1)$. Hence

$$\sum_{\mathfrak{a}\mathbf{N}\mathfrak{a}\le n} \vartheta(\mathfrak{a})\mathbf{N}\mathfrak{a}^{-\sigma} = \Theta(1) + \sum_{k=2}^{n} \left[\Theta(k) - \Theta(k-1)\right] k^{-\sigma}$$

Collecting the terms with a factor $\Theta(k)$ we get

$$= \sum_{k=1}^{n-1} \Theta(k)\left[k^{-\sigma} - (k+1)^{-\sigma}\right] + \Theta(n)n^{-\sigma}$$

which converges to $\sum_{n=1}^{\infty} \Theta(n)\left[n^{-\sigma} - (n+1)^{-\sigma}\right]$ for $\mathrm{Re}(\sigma) > 1$. Hence for real $\sigma > 1$

$$S(\sigma) = \sum_{n=1}^{\infty} \Theta(n)\left[n^{-\sigma} - (n+1)^{-\sigma}\right]$$

and likewise

$$T(\sigma) = \sum_{n=1}^{\infty} H(n)\left[n^{-\sigma} - (n+1)^{-\sigma}\right].$$

For a given $\epsilon > 0$, let $n_0$ be such that for all $n > n_0$

$$\left|\frac{\Theta(n)}{H(n)} - d\right| < \epsilon.$$

We then get for $\sigma > 1$ that

$$\begin{aligned}
\left|\frac{S(\sigma)}{T(\sigma)} - d\right| &= \frac{1}{T(\sigma)}\left|\frac{S(\sigma) - dT(\sigma)}{T(\sigma)}\right| \\
&= \frac{1}{T(\sigma)}\left|\sum_{n=1}^{\infty}[\Theta(n) - dH(n)]\left[n^{-\sigma} - (n+1)^{-\sigma}\right]\right| \\
&\le \frac{1}{T(\sigma)}\left(\left|\sum_{n=1}^{n_0}[\Theta(n) - dH(n)]\left[n^{-\sigma} - (n+1)^{-\sigma}\right]\right|\right. \\
&\left. + \left|\sum_{n=n_0+1}^{\infty}[\Theta(n) - dH(n)]\left[n^{-\sigma} - (n+1)^{-\sigma}\right]\right|\right) \\
&\le \frac{1}{T(\sigma)}\left(\sum_{n=1}^{n_0}|\Theta(n) - dH(n)|\left[n^{-\sigma} - (n+1)^{-\sigma}\right]\right. \\
&\left. + \sum_{n=n_0+1}^{\infty}|\Theta(n) - dH(n)|\left[n^{-\sigma} - (n+1)^{-\sigma}\right]\right) \\
&\le \frac{1}{T(\sigma)}\left(\sum_{n=1}^{n_0}|\Theta(n) - dH(n)|\left[n^{-\sigma} - (n+1)^{-\sigma}\right]\right. \\
&\left. + \epsilon\sum_{n=n_0+1}^{\infty}H(n)\left[n^{-\sigma} - (n+1)^{-\sigma}\right]\right) \\
&= \frac{1}{T(\sigma)}\sum_{n=1}^{n_0}|\Theta(n) - dH(n)|\left[n^{-\sigma} - (n+1)^{-\sigma}\right] \\
&+ \frac{1}{T(\sigma)}\epsilon\sum_{n=n_0+1}^{\infty}H(n)\left[n^{-\sigma} - (n+1)^{-\sigma}\right]
\end{aligned}$$

The first term goes to zero as $\sigma \to 1$, since it is a finite sum for every $\sigma$ divided by $T(\sigma)$, which behaves in the limit to 1 as $\log((\sigma - 1)^{-1})$ by theorem 5.1. Hence $\sigma$ close enough to one the first term is smaller than $\epsilon$. The second term is bounded by $\epsilon$, since the sum consists of positive terms all of which occur in the series of positive terms $T(\sigma)$. Hence we get

$$\le 2\epsilon.$$

Hence $M$ has Dirichlet density equal to $d$.

**Theorem 5.4 (Chebotarev's Density Theorem)** *Let $F/K$ be a finite Galois extension of number fields. Let $\mathcal{C}$ be a conjugacy class of* $\mathrm{Gal}(F/K)$*. Then*

$$S_{\mathcal{C}} = \{\mathfrak{p} \textit{ unramified in } F/K \textit{ such that } \mathrm{Frob}_{\mathfrak{p}} \in \mathcal{C}\}$$

*has Dirichlet density*

$$\frac{\#\mathcal{C}}{\#\operatorname{Gal}(F/K)}.$$

Proof We wish to compute the Dirichlet density of $S_{\mathcal{C}}$, which is by definition

$$\lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S_{\mathcal{C}}} \mathbf{N}\mathfrak{p}^{-s}}{\log(1/(s-1))}$$

Set

$$f(s) = \sum_{\mathfrak{p}\in S_{\mathcal{C}}} \mathbf{N}\mathfrak{p}^{-s}.$$

Set $C_{\mathcal{C}}\colon \operatorname{Gal}(F/K) \to \mathbf{C}$ as

$$C_{\mathcal{C}}(g) = \begin{cases} 1 & \text{if } g \in \mathcal{C}, \\ 0 & \text{otherwise.} \end{cases}$$

Then $C_{\mathcal{C}}$ is a class function, and

$$\begin{aligned} f(s) &= \sum_{\mathfrak{p}\in S_{\mathcal{C}}} \mathbf{N}\mathfrak{p}^{-s} \\ &= \sum_{\mathfrak{p} \text{ unramified}} C_{\mathcal{C}}(\operatorname{Frob}_{\mathfrak{p}})\mathbf{N}\mathfrak{p}^{-s} \\ &\overset{3.36}{=} \sum_{\substack{\mathfrak{p} \text{ unramified} \\ \rho}} \langle \chi_\rho, C_{\mathcal{C}}\rangle \chi_\rho(\operatorname{Frob}_{\mathfrak{p}})\mathbf{N}\mathfrak{p}^{-s} \end{aligned}$$

Define

$$f_\rho(s) = \sum_{\mathfrak{p} \text{ unramified}} \chi_\rho(\operatorname{Frob}_{\mathfrak{p}})\mathbf{N}\mathfrak{p}^{-s}.$$

We then see that $f(s)$ is equal to

$$\begin{aligned} &= \sum_\rho \langle \chi_\rho, C_{\mathcal{C}}\rangle f_\rho(s) \\ &= \frac{\#\mathcal{C}}{\#\operatorname{Gal}(F/K)} f_{\mathbf{1}}(s) + \sum_{\rho\neq\mathbf{1}} \langle \chi_\rho, C_{\mathcal{C}}\rangle f_\rho(s). \end{aligned}$$

We will now show that the second term is bounded. The factor in the first term is the density that we wanted. We see that the limit we are interested in is equal to

$$\lim_{s\to 1} \frac{\sum_{\mathfrak{p}\in S_{\mathcal{C}}} \mathbf{N}\mathfrak{p}^{-s}}{\log 1/(s-1)} = \lim_{s\to 1} \frac{\left(\frac{\#\mathcal{C}}{\#\operatorname{Gal}(F/K)} f_{\mathbf{1}}(s) + \sum_{\rho\neq\mathbf{1}} \langle \chi_\rho, C_{\mathcal{C}}\rangle f_\rho(s)\right)}{\log(1/(s-1))} \tag{5.1}$$

We will compute the limit on the right hand side by showing that the asymptotic behaviour of the $f_\rho(s)$ is the same as $L_{\mathfrak{c}}(\rho, s)$ for a suitable cycle $\mathfrak{c}$. Let $\rho$ be a representation of $\mathrm{Gal}(F/K)$. Let $\mathfrak{c}$ be the product of all primes of $K$ which ramify in $F$. Then by theorem 4.38 (here $L_{\mathfrak{c}} = L_*$) we know that

$$\begin{aligned}&L_{\mathfrak{c}}(\rho, s) \neq 0, \infty \text{ at } s = 1 \text{ if } \rho \neq \mathbf{1} \text{ irreducible,}\\ &L_{\mathfrak{c}}(\mathbf{1}, s) \text{ has a simple pole at } s = 1.\end{aligned}$$

Since $\mathfrak{p}$ is unramified in $F/K$, we have $I_{\mathfrak{p}} = \{e\}$ , hence $\rho^{I_{\mathfrak{p}}} = \rho$. Let the eigenvalues of $\mathrm{Frob}_{\mathfrak{p}}$ acting on the representation space via $\rho$ be $\lambda_1, \ldots, \lambda_d$ (with multiplicity). Recall that $P_{\mathfrak{p}}$ is the local polynomial (see definition 4.16). Then

$$\begin{aligned}\log \frac{1}{P_{\mathfrak{p}}(\rho, \mathbf{N}\mathfrak{p}^{-s})} &= \log \frac{1}{\prod_i 1 - \lambda_i \mathbf{N}\mathfrak{p}^{-s}}\\ &= \sum_i \log \frac{1}{1 - \lambda_i \mathbf{N}\mathfrak{p}^{-s}}\\ &= \left(\sum_i \lambda_i\right) \mathbf{N}\mathfrak{p}^{-s} + \frac{(\sum_i \lambda_i^2)}{2} \mathbf{N}\mathfrak{p}^{-2s} + \cdots\\ &= \sum_{n \geq 1} \frac{\chi_\rho(\mathrm{Frob}_{\mathfrak{p}}^n)}{n} \mathbf{N}\mathfrak{p}^{-ns}\end{aligned}$$

Consider

$$\sum_{\mathfrak{p} \text{ unramified}} \sum_{n \geq 1} \frac{\chi_\rho(\mathrm{Frob}_{\mathfrak{p}}^n)}{n} \mathbf{N}\mathfrak{p}^{-ns}.$$

As a Dirichlet series, its coefficients are sums of the various $\chi_\rho(\mathrm{Frob}_{\mathfrak{p}}^n)/n$. These are bounded, since $\chi$ is a character. Moreover, as a Dirichlet series $\sum a_n/n^s$, every $n$ is equal to some $p^\mu$, since $\mathbf{N}\mathfrak{p}^n = p^{fn}$ where $f$ is the residue degree of $\mathfrak{p}$. There are at most $[K : \mathbf{Q}]$ primes $\mathfrak{p}$ over $p$. Hence at most $[K : \mathbf{Q}]$ contribute to each coefficient. We see that the coefficients are bounded, and hence that this Dirichlet series defines an analytic branch of $\log(L_{\mathfrak{c}}(\rho, s))$ on $\mathrm{Re}(s) > 1$. Denote this analytic branch also by $\log(L_{\mathfrak{c}}(\rho, s))$.

Note that

$$f_\rho(s) = \log(L_{\mathfrak{c}}(\rho, s)) - \sum_{\mathfrak{p} \text{ unramified}} \sum_{n \geq 2} \frac{\chi(\mathrm{Frob}_{\mathfrak{p}}^n)}{n} \mathbf{N}\mathfrak{p}^{-ns}$$

We wish to show that the asymptotic behaviour of $f_\rho(s)$ and $\log(L_{\mathfrak{c}}(\rho, s))$ for $s \to 1$ is the same, and we do this by showing that the second term in the above expression for $f_\rho(s)$ is bounded. Note that for a prime $p \in \mathbf{Z}$ there are at most

$[K : \mathbf{Q}]$ primes $\mathfrak{p}$ of $K$ over $p$. Hence for $\mathrm{Re}(s) > 1$

$$\begin{aligned}
|\log(L_{\mathfrak{c}}(\rho, s)) - f_\rho(s)| &= \left| \sum_{\mathfrak{p} \text{ unramified}} \sum_{n \geq 2} \frac{\chi(\mathrm{Frob}_{\mathfrak{p}}^n)}{n} \mathbf{N}\mathfrak{p}^{-ns} \right| \\
&\leq \sum_{\mathfrak{p} \text{ unramified}} \sum_{n \geq 2} \left| \frac{\chi(\mathrm{Frob}_{\mathfrak{p}}^n)}{n} \mathbf{N}\mathfrak{p}^{-ns} \right| \\
&\leq \dim \rho \cdot \sum_{\mathfrak{p} \text{ unramified}} \sum_{n \geq 2} \left| \frac{1}{n} \mathbf{N}\mathfrak{p}^{-ns} \right| \\
&\leq \dim \rho \cdot \sum_{\mathfrak{p} \text{ unramified}} \sum_{n \geq 2} \left| \frac{1}{\mathbf{N}\mathfrak{p}^{ns}} \right| \\
&\leq \dim \rho \cdot [K : \mathbf{Q}] \cdot \sum_{\substack{p \in \mathbf{Z} \\ \text{prime}}} \sum_{n \geq 2} \frac{1}{|p^s|^n} \\
&= \dim \rho \cdot [K : \mathbf{Q}] \cdot \sum_{\substack{p \in \mathbf{Z} \\ \text{prime}}} \frac{1}{|p^s|^2} \frac{1}{1 - |1/p^s|} \\
&= \dim \rho \cdot [K : \mathbf{Q}] \cdot \sum_{\substack{p \in \mathbf{Z} \\ \text{prime}}} \frac{1}{|p^s|(|p^s| - 1)} \\
&\leq \dim \rho \cdot [K : \mathbf{Q}] \cdot \sum_{\substack{p \in \mathbf{Z} \\ \text{prime}}} \frac{1}{|p|^{\mathrm{Re}(s)}(|p|^{\mathrm{Re}(s)} - 1)} \\
&\leq \dim \rho \cdot [K : \mathbf{Q}] \cdot \sum_{\substack{p \in \mathbf{Z} \\ \text{prime}}} \frac{1}{|p|(|p| - 1)} \quad (\text{as } \mathrm{Re}(s) > 1) \\
&\leq \dim \rho \cdot [K : \mathbf{Q}] \cdot \sum_{\substack{p \in \mathbf{Z} \\ \text{prime}}} \frac{1}{(|p| - 1)^2} \quad (\text{as } \mathrm{Re}(s) > 1) \\
&\leq \dim \rho \cdot [K : \mathbf{Q}] \cdot \sum_{k=1}^{\infty} \frac{1}{k^2} \\
&< \infty.
\end{aligned}$$

So

$$f_\rho(s) = \sum_{\mathfrak{p} \text{ unramified}} \chi_\rho(\mathrm{Frob}_{\mathfrak{p}}) \mathbf{N}\mathfrak{p}^{-s}$$

is bounded as $s \to 1$ on $\mathrm{Re}(s) > 1$ if $\rho \neq \mathbf{1}$ irreducible and

$$f_{\mathbf{1}}(s) = \sum_{\mathfrak{p} \text{ unramified}} \mathbf{N}\mathfrak{p}^{-s} \sim \log \frac{1}{s-1}$$

as $s \to 1$.

Using these two asymptotic results in eq. (5.1) gives the desired result. $\blacksquare$

**Remark 5.5** Once can show that the set of primes has in fact a natural density. Then proposition 5.3 and theorem 5.4 combined show that this natural density is then equal to $\#\mathcal{C}/\#G$. The interested reader is referred to Serre [10, I-26.A.3].

# Part II

# Preliminaries on elliptic curves

# Introduction

In this chapter we will state what we will need from the theory of elliptic curves. For an extensive treatment of elliptic curves we refer to Silverman and Tate [15] and Silverman [14]. Most of the references are to the second book. Basic terminology and concepts from algebraic geometry as covered in chapter I and II from Silverman [14] are also freely used.

The field over which we work is denoted by $K$ (and typically is $\mathbf{Q}$, a number field, a local field $K_{\mathfrak{p}}$, or a finite field).

Consider the general cubic equation in two variables $x$ and $y$:

$$E : ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0. \tag{5.2}$$

Such an equation defines a projective curve. If the curve is smooth the genus turns out to be one. What is more, every curve of genus one is isomorphic to a cubic curve as above (Silverman [14, proposition III.3.1]).

**Definition 5.6** A pair $(E, O)$ with $E$ a smooth projective curve of genus one over a field $K$ and $O \in E(K)$ is called an **elliptic curve**. To express the fact that $E$ is defined over $K$ we also write $E/K$. Equivalently, an elliptic curve is the zero locus of a cubic equation as in eq. (5.2) with a so called **base point** $O$ which is a solution to eq. (5.2). Often we suppress the $O$ and just write $E$ for an elliptic curve.

There is a geometric way to define a group law on any elliptic curve. Using the resulting group structure one can learn a lot about an elliptic curve, for example formulas for the number of points on an elliptic curve.

# Chapter 6

# Elliptic curves

## 6.1 Weierstrass equations

As shown in Silverman and Tate [15, I.3], by choosing suitable axes in projective space, eq. (5.2) can be transformed into the following form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

such that the base point $O$ is the projective point $[0, 1, 0]$ at infinity. This is called a **Weierstrass equation** for $E$. If $\mathrm{char}(K) \neq 2$ then we can, as in Silverman [14, III.1], use the substitution

$$y \mapsto \frac{1}{2}(y - a_1x - a_3)$$

and completing the square then gives an equation of the form

$$E : y^2 = 4x^3 + b_2x^3 + 2b_4x + b_6,$$

where

$$b_2 = a_1^4 + 4a_4, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

This is also called a **Weierstrass equation** for $E$. We define the quantities

$$\begin{aligned}
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\
c_4 &= b_2^2 - 24b_4, \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.
\end{aligned}$$

If $\mathrm{char}(K) \neq 2, 3$ then the substitution

$$(x, y) \mapsto (\frac{x - 3b_2}{36}, \frac{y}{108})$$

eliminates the $x^2$ term, yielding the simpler equation

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

**Definition 6.1** The quantity $\Delta$ is called the discriminant of the Weierstrass equation.

**Proposition 6.2** *The curve given by a Weierstrass equation is nonsingular if and only if $\Delta \neq 0$.*

Proof See Silverman [14, proposition III.1.4.(a).(i)]. ∎

## 6.2 Group law

**Definition 6.3** Let $E$ be an elliptic curve. Let $P, Q \in E$, and let $L$ be the line through these two points (the line through two points on $E$ that coincide is taken to be the tangent at $E$ at that one point). Let $R'$ be the third point of intersection of $L$ with $E$. Let $L'$ be the line through $R'$ and $O$ and let $R$ be the third point of intersection of $L'$ with $E$. Then the operation $+$ on $E$ is defined by $P + Q = R$, and this notation is justified by the following proposition.

**Proposition 6.4** *The operation $+$ turns $E$ into an abelian group.*

Proof See Silverman [14, proposition III.2.2]. ∎

**Remark 6.5** When a curve is given by a Weierstrass equation we will always take for $O$ the point at infinity $[0, 1, 0]$ on $E$.

**Proposition 6.6** *If $E$ is the elliptic curve defined by the Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

*over a field $K$, then for every algebraic extension $L/K$ the set*

$$E(K) = \{(x, y) \in L^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

*is a subgroup of $E = E(\overline{K})$, where $\overline{K}$ denotes the algebraic closure of $K$.*

Proof See Silverman [14, proposition III.2.2.(f)]. ∎

**Notation 6.7** For $m \in \mathbf{Z}$ we write

$$[m]P = \begin{cases} \underbrace{P + \cdots + P}_{m \text{ times}} & \text{if } m > 0, \\ \underbrace{-P - \cdots - P}_{|m| \text{ times}} & \text{if } m < 0, \\ [0]P = O & \text{if } m = 0. \end{cases}$$

**Remark 6.8** When $E$ is given by a Weierstrass equation there are explicit formulas for the coordinates of $P + Q$ in terms of the coordinates of $P$ and $Q$, see Silverman [14, section III.2].

## 6.3 Points of finite order

When $A$ is an abelian group and $m$ an integer, we denote by $A[m]$ the $m$-torsion of $A$, that is, the subgroup of elements $a$ of $A$ such that $ma = 0$. Equivalently, $A[m]$ is the kernel of the multiplication by $m$ map $A \to A\colon a \mapsto ma$. In the case of elliptic curves, there is a structure theorem for the torsion group $E[m]$. The proof of this structure theorem uses, among other things, the notions of differentials, separable morphisms, isogenies, dual isogenies and the degree of a map. We refer to Silverman [14] for a coverage of these notions, in particular sections III.3 to III.6. The conclusion is

**Corollary 6.9** *Let $E$ be an elliptic curve and let $m \in \mathbf{Z}$ with $m \neq 0$.*

*(a) If $m \neq 0$ in $K$, i.e. if either* $\operatorname{char}(K) \neq 0$ *or* $\operatorname{char}(K) > 0$ *and*

$$\operatorname{char}(K) \nmid m,$$

*then*

$$E[m] \cong \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}.$$

*(b) If* $\operatorname{char}(K) = p > 0$*, then one of the following is true:*

*(i) $E[p^e] \cong \{O\}$ for all $e = 1, 2, 3, \ldots$,*

*(ii) $E[p^e] \cong \mathbf{Z}/p^e\mathbf{Z}$ for all $e = 1, 2, 3, \ldots$.*

Given two points $P$ and $Q$ on an elliptic curve $E$ there is an algebraic expression for the coordinates of $P + Q$. In particular, this is true for $P = Q$. Hence the coordinates of $P + P$ are expressible algebraically in terms of those of $P$. One can iterate this and express the coordinates of $P + (P + P)$ algebraically in terms of those of $P$ and $P + P$, but the coordinates of $P + P$ were expressible algebraically in terms of the coordinates of $P$. Continuing in this fashion we see that the coordinates of $[m]P$ for $m \in \mathbf{Z}$ are expressible algebraically in terms of the coordinates of $P$. The exact expression is derived in exercise III.3.7 of Silverman [14]. This shows that if we have an elliptic curve $E$ over a field $K$ and an integer $m$ and we add to $K$ all the $x$-coordinates of the $m$-torsion points on $E$ then this gives a finite algebraic extension of $K$. Because of the Weierstrass equation, adding all the $y$-coordinates, which amounts to adding some square roots, again gives a finite algebraic extension. We denote this extension by $K(E[m])/K$.

## 6.4 Reducing elliptic curves

We treat parts of Silverman [14, section VII.1 and section VII.2]. We use the following notation, as in Silverman [14, chapter VII]:

- $K$ is a local field, complete with respect to a discrete valuation $v$.
- $R = \{x \in K : v(x) \geq 0\}$, the ring of integers of $K$.

- $R^* = \{x \in K : v(x) = 0\}$, the unit group of $R$.
- $\mathfrak{m} = \{x \in K : v(x) > 0\}$, the maximal ideal of $R$.
- $\pi$ a uniformizer for $R$, i.e., $\mathfrak{m} = \pi R$.
- $k = R/\mathfrak{m}$, the residue field of $R$.

Assume that $v$ is normalized so that $v(\pi) = 1$.

Let $E/K$ be an elliptic curve satisfying a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The substitution $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ leads to a new Weierstrass equation in which $a_i$ is replaced by $u^ia_i$, so by choosing $u$ divisible by a high enough power of $\pi$ we get an equation with all coefficients $a_i$ lying in $R$. Then the discriminant of this equation satisfies $v(\Delta) > 0$. The valuation, being discrete, attains a minimal value over all such equations with coefficients in $R$.

**Definition 6.10** Let $E/K$ be an elliptic curve. A Weierstrass equation for $E$ is called a **minimal (Weierstrass) equation for $E$ at $v$** if $v(\Delta)$ is minimized subject to the condition that the $a_i$ are in $R$. This minimal value of $v(\Delta)$ is called the **valuation of the minimal discriminant of $E$ at $v$**.

**Proposition 6.11** *(a) Every elliptic curve $E/K$ has a minimal Weierstrass equation.*

*(b) A minimal Weierstrass equation is unique up to a change of coordinates*

$$x = u^2x' + r, \quad y = x^3y' + u^2sx' + t$$

*with $u \in R^*$ and $r, s, t \in R$.*

Proof See Silverman [14, VII.2.1.3]. ∎

Denote the map $R \to R/\pi R = k$ by a tilde: $t \mapsto \tilde{t}$. After choosing a minimal Weierstrass equation for $E/K$, we can reduce its coefficients modulo $\pi$ to obtain a possibly singular elliptic curve over $k$, namely

$$\tilde{E} : y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6.$$

The curve $\tilde{E}/k$ is called the **reduction of $E$ modulo $\pi$**.

Let $P = [x_0, y_0, z_0] \in E(K)$. By multiplying the coordinates with a suitable power of $\pi$, we can assume that all the coefficients of $P$ are in $R$ and at least one is in $R^*$. Then the reduced point

$$\tilde{P} = [\tilde{x}_0, \tilde{y}_0, \tilde{z}_0]$$

is in $\tilde{E}(k)$. This defines the **reduction map**

$$E(K) \to \tilde{E}(k), P \mapsto \tilde{P}.$$

Note that if $\Delta$ is the discriminant of the minimal Weierstrass equation for $E$, then $\tilde{\Delta} = 0$ if and only if $v(\Delta) > 0$. In case $\tilde{E}$ is non-singular we say that $E$ has **good reduction** at $v$.

The case of so called **bad reduction** can also be of interest. For more on this we refer to Silverman [14, VII.5].

Suppose $E$ is an elliptic curve over a number field $K$, and $v$ is a prime of $K$. We then say that $E$ has **good reduction at** $v$ if it has good reduction at $v$ when considered as an elliptic curve over the local field $K_v$.

## 6.5 Neron-Ogg-Shafarevich criterion

We have the following criterion by Néron, Ogg and Shafarevich regarding the ramification of $K(E[m])/K$ in the case $K$ is a local field.

**Theorem 6.12 (Néron-Ogg-Shafarevich)**
*Let $E/K$ be an elliptic curve with $K$ a local field, $v$ its valuation, $k$ its residue field, $m$ an integer prime to* char$(k)$*. Then $K(E[m])/K$ is unramified if and only if $E$ has good reduction at $v$.*

Proof See Silverman [14, exercise VII.7.9.(b)] ■

**Corollary 6.13** *Let $E/\mathbf{Q}$ be an elliptic curve, with discriminant $\Delta_E$. Let $m$ be an integer, $p$ a prime of $\mathbf{Q}$ with $p$-adic valuation $v_p$ such that $v_p(m) = v_p(\Delta_E) = 0$. Then $\mathbf{Q}(E[m])/\mathbf{Q}$ is unramified at $p$.*

Proof Localize at $p$ and apply theorem 6.12. ■

## 6.6 The Tate module

**Definition 6.14** Let $E/K$ be an elliptic curve, let $\ell \in \mathbf{Z}$ be a prime such that $\ell \neq \mathrm{char}(K)$. The **($\ell$-adic) Tate module** of $E$ is the profinite group

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

the inverse limit being taken with respect to the natural maps

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n].$$

Since each $E[\ell^n]$ is a $\mathbf{Z}/\ell^n\mathbf{Z}$-module, the Tate module has a natural structure as a $\mathbf{Z}_\ell$-module. Furthermore, since the multiplication-by-$\ell$ maps are surjective, every basis $\{P_n, Q_n\}$ of $E[\ell^n]$ can be lifted to a basis $\{P_{n+1}, Q_{n+1}\}$ of $E[\ell^{n+1}]$, where the fact that it's lifted means that $[l]P_{n+1} = P_n$ and $[l]Q_{n+1} = Q_n$. (Use induction to see this.) Using this, we see that as topological groups

$$\begin{aligned} T_\ell(E) &\cong \varprojlim_n (\mathbf{Z}/\ell^n\mathbf{Z} \times \mathbf{Z}/\ell^n\mathbf{Z}) \\ &\cong \varprojlim_n \mathbf{Z}/\ell^n\mathbf{Z} \times \varprojlim_n \mathbf{Z}/\ell^n\mathbf{Z} \\ &\cong \mathbf{Z}_\ell \times \mathbf{Z}_\ell. \end{aligned}$$

Hence we have proved:

**Proposition 6.15** *As a $\mathbf{Z}_\ell$-module, the Tate-module has the following structure, if $\ell \neq \mathrm{char}(K)$,*

$$T_\ell(E) \cong \mathbf{Z}_\ell \times \mathbf{Z}_\ell.$$

The action of $G_{\overline{K}/K}$ on each $E[\ell^n]$ commutes with the multiplication-by-$\ell$ map used to form the inverse limit, so $G_{\overline{K}/K}$ also acts on $T_\ell(E)$. Since the profinite group $G_{\overline{K}/K}$ acts continuously on each finite (discrete) group $E[\ell^n]$, the resulting action on $T_\ell(E)$ is also continuous.

**Definition 6.16** The **$\ell$-adic representation (of $G_{\overline{K}/K}$) associated to $E$** is the homomorphism

$$\rho_\ell \colon G_{\overline{K}/K} \to \mathrm{Aut}(T_\ell(E))$$

induced by the action of $G_{\overline{K}/K}$ on $E[\ell^n]$.

# Chapter 7

# Elliptic curves over finite fields

## 7.1 The action of the Frobenius map on an elliptic curve

**Definition 7.1** Let $V \subset \mathbf{P}^n$ be a variety defined over a finite field $\mathbf{F}_q$. The $q$-th power map

$$\varphi_q = [X_0^q : \ldots : X_n^q]$$

is a morphism $\varphi : V \to V$ called the **Frobenius morphism**.

## 7.2 The zeta function of an elliptic curve

**Definition 7.2** Let $E/\mathbf{F}_q$ be an elliptic curve. The **zeta function** of $E/\mathbf{F}_q$ is defined by the power series

$$Z(E/\mathbf{F}_q; T) = \exp\left(\sum_{n=1}^{\infty} (\#E(\mathbf{F}_q)) \frac{T^n}{n}\right).$$

Note that if we know the zeta function of an elliptic curve we can determine all the $\#E(\mathbf{F}_q)$ by differentiating $n$ times and plugging in $T = 0$. We have the Weil conjectures for these zeta functions of elliptic curves (Silverman [14, V.2.4]):

**Theorem 7.3 (Weil Conjectures for elliptic curves)** *Let $E/\mathbf{F}_q$ be an elliptic curve. Then there is an $a \in \mathbf{Z}$ such that*

$$Z(E/\mathbf{F}_q; T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}.$$

*Furthermore,*

$$Z(E/\mathbf{F}_q; 1/qT) = Z(E/\mathbf{F}_q; T),$$

*and*

$$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T) \text{ with } |\alpha| = |\beta| = \sqrt{q}.$$

**Remark 7.4** Note that the above rational form for the zeta function only depends on $a$. Differentiating once and plugging in $T = 0$ shows that $\#E(\mathbf{F}_q) = -a+1+q$, hence the zeta function is completely determined by $\#E(\mathbf{F}_q)$. Hence $\#E(\mathbf{F}_q)$ determines all $E(\mathbf{F}_{q^n})$ for all $n \in \mathbf{N}$.

Does the converse also hold? That is, does $\#E(\mathbf{F}_{q^n})$ for some $n \geq 2$ also always determine $\#E(\mathbf{F}_q)$? The answer is no, as the following counterexample shows.

**Example 7.5** Consider the elliptic curves over $\mathbf{F}_3$ given by

$$\begin{aligned} E_1 &: y^2 = x^3 + 2x + 1 \\ E_2 &: y^2 = x^3 + 2x + 2 \end{aligned}$$

Then $\#E_1(\mathbf{F}_9) = \#E_2(\mathbf{F}_9) = 7$, but $\#E_1(\mathbf{F}_3) = 1$ and $\#E_2(\mathbf{F}_3) = 7$.

## 7.3 The number of points as traces

We need the following point counting formula for elliptic curves.

**Remark 7.6 (Silverman [14], Remark V.2.6)**
Let $E/\mathbf{F}_q$ be an elliptic curve. The quantity

$$a = q + 1 - \#E(\mathbf{F}_q)$$

is called the **trace of Frobenius**, because by Silverman and Tate [15, V.2.6] it is equal to the trace of the $q$-power Frobenius map considered as a linear transformation of $T_\ell(E)$. This linear transformation is denoted $\varphi_\ell$. Thus if $\varphi$ denotes the $q$-power Frobenius map, then

$$a = 1 + q - \#E(\mathbf{F}_q) = \mathrm{Tr}(\varphi_\ell)$$

To get a better feeling for the formula

$$\mathrm{Tr}(\varphi_\ell) = 1 + q - \#E(\mathbf{F}_q)$$

we calculate an explicit example. The computations were done with the help of SAGE. Consider the curve

$$E : y^2 = x^3 + 2x + 1$$

over $\mathbf{F}_5$. Represent the field $\mathbf{F}_{5^{24}}$ by $\mathbf{F}_5(t)$ with $t$ satisfying the reducible equation

$$\begin{aligned}&t^{24}+2t^{16}+4t^{15}+4t^{13}+2t^{12}+t^{11}\\&+3t^{10}+4t^{8}+2t^{7}+4t^{6}+2t^{4}+3t^{3}+3t^{2}+t+2=0.\end{aligned}$$

As an abelian group, $E(\mathbf{F}_{5^{24}})$ is isomorphic to $\mathbf{Z}/2016\mathbf{Z}\oplus\mathbf{Z}/29565795863520\mathbf{Z}$, with generators

$$\begin{aligned}P=(&2t^{23}+4t^{22}+4t^{21}+4t^{19}+4t^{17}+t^{15}+4t^{14}+4t^{13}+t^{12}+2t^{11}\\&+t^{10}+t^{9}+2t^{7}\\&+3t^{6}+2t^{4}+4t^{3}+4t+2,\\&3t^{23}+2t^{22}+3t^{21}+3t^{20}+2t^{19}+3t^{18}+4t^{17}+4t^{16}+4t^{15}+4t^{14}\\&+2t^{13}+3t^{11}\\&+3t^{10}+t^{8}+t^{7}+2t^{6}+t^{5}+2t^{3}+t^{2}+4t+2)\\Q=(&t^{23}+4t^{22}+3t^{21}+3t^{20}+2t^{19}+4t^{17}+t^{16}+t^{15}+4t^{14}+t^{13}\\&+3t^{12}+4t^{9}+t^{8}\\&+3t^{7}+3t^{6}+4t^{5}+4t^{4}+2t^{3}+4t^{2}+t+3\\&2t^{23}+2t^{22}+t^{21}+3t^{20}+t^{19}+4t^{18}\\&+4t^{17}+2t^{16}+2t^{14}+t^{13}+t^{12}+4t^{11}+2t^{10}+4t^{9}+4t^{7}+t^{6}+t^{5}+t^{4}+t^{3}\\&+4t^{2}+2t+3)\end{aligned}$$

of order 2016 and 29565795863520 respectively. These orders have prime factorization

$$\begin{aligned}2016&=2^5\cdot 3^2\cdot 7,\\29565795863520&=2^5\cdot 3^2\cdot 5\cdot 7\cdot 17\cdot 73\cdot 229\cdot 10321,\end{aligned}$$

hence

$$\begin{aligned}e_1&=[3^2\cdot 7]P,\\e_2&=[3^2\cdot 5\cdot 7\cdot 17\cdot 73\cdot 229\cdot 10321]Q,\end{aligned}$$

are two distinct elements of order $2^5=32$, hence they generate

$$E[32]=\langle e_1,e_2\rangle$$

as a $\mathbf{Z}/32\mathbf{Z}$-module. A calculation shows that applying the Frobenius automorphism $\varphi\colon E[32]\to E[32]$ to these generators yields

$$\begin{aligned}\varphi(e_1)&=17e_1+3e_2,\\\varphi(e_2)&=3e_1+14e_2,\end{aligned}$$

hence $\varphi$ has matrix

$$M_{\varphi,32} = \begin{pmatrix} 17 & 3 \\ 3 & 14 \end{pmatrix}$$

with respect to the basis $e_1, e_2$. This matrix has trace 31 (mod 32). According to our formula, this implies that

$$\begin{aligned} \#E(\mathbf{F}_5) &= 1 + 5 - \mathrm{Tr}(\varphi_2) \\ &\equiv -25 \pmod{32} \\ &\equiv 7 \pmod{32}. \end{aligned}$$

But since $0 \leq \#E(\mathbf{F}_5) \leq 5^2 + 1 = 26$, we see that in fact $\#E(\mathbf{F}_5) = 7$. One easily verifies that $E(\mathbf{F}_5)$ has indeed this number of points:

$$\begin{aligned} E(\mathbf{F}_5) = \{&(0:1:0), (0:1:1), (0:4:1), (1:2:1), \\ &(1:3:1), (3:2:1), (3:3:1)\}. \end{aligned}$$

We do it again, but this time by computing a matrix representation of the action of the Frobenius on $E[64]$ with respect to a basis that lifts the basis $\{e_1, e_2\}$ of $E[32]$. To this end, we let SAGE compute that considered over $\mathbf{F}_{5^{48}}$ the elliptic curve $E$ is isomorphic to

$$\mathbf{Z}/2124864\mathbf{Z} \oplus \mathbf{Z}/16719722668370780198794281 60\mathbf{Z},$$

as an abelian group, and that

$$\begin{aligned} 2124864 &= 2^6 \cdot 3^2 \cdot 7 \cdot 17 \cdot 31 \text{ and} \\ 1671972266837078019879428160 &= 2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17 \cdot 31 \cdot 73 \cdot 229 \cdot 5953 \\ &\quad \cdot 6673 \cdot 10321 \cdot 22961, \end{aligned}$$

Over $\mathbf{F}_{5^{48}}$ we find all the 64-torsion of $E$. We represent the field $\mathbf{F}_{5^{48}}$ by $\mathbf{F}_5(s)$ with

$$\begin{aligned} s^{48} + 2\cdot s^{47} + 2\cdot s^{46} + 2\cdot s^{45} + 2\cdot s^{44} + 3\cdot s^{43} + s^{42} + 2\cdot s^{41} + \\ 4\cdot s^{40} + 3\cdot s^{39} + 2\cdot s^{38} + 3\cdot s^{37} + 2\cdot s^{36} + 4\cdot s^{35} + s^{34} + s^{33} + s^{32} \\ +4\cdot s^{30} + s^{29} + 3\cdot s^{28} + 3\cdot s^{27} + 3\cdot s^{26} + s^{25} + 2\cdot s^{22} + 4\cdot s^{21} + \\ 2\cdot s^{19} + 4\cdot s^{18} + 2\cdot s^{17} + 3\cdot s^{15} + 4\cdot s^{14} + 3\cdot s^{13} + 4\cdot s^{12} + 4\cdot s^{11} + \\ s^{10} + 2\cdot s^{9} + 2\cdot s^{8} + 4\cdot s^{7} + 3\cdot s^{6} + 2\cdot s^{5} + s^{3} + 3 = 0 \end{aligned}$$

We embed our representation of $\mathbf{F}_{5^{24}}$ in our representation of $\mathbf{F}_{5^{48}}$ by sending $t$ to one of the zeroes of the minimal polynomial $f^{t}_{\mathbf{F}_5}$ in $F_5(s)$, namely

$$\begin{aligned}
-(s^{46} + 2\cdot s^{45} + 2\cdot s^{44} + 3\cdot s^{43} + 2\cdot s^{42} + 3\cdot s^{41} + 2\cdot s^{39} + 3\cdot s^{38}\\
+4\cdot s^{37} + 4\cdot s^{36} + 3\cdot s^{35} + 3\cdot s^{34} + 4\cdot s^{33} + s^{32} + 2\cdot s^{29} + 4\cdot s^{28} +\\
s^{27} + 3\cdot s^{26} + 2\cdot s^{25} + s^{24} + 4\cdot s^{22} + 3\cdot s^{20} + s^{18} + 3\cdot s^{16} + 4\cdot s^{15}\\
+2\cdot s^{14} + 4\cdot s^{12} + s^{11} + s^{10} + 3\cdot s^{9} + s^{8} + 2\cdot s^{7} + s^{6} + 3\cdot s^{5} +\\
3\cdot s^{4} + 2\cdot s^{3} + 2\cdot s^{2} + 4\cdot s)
\end{aligned}$$

This yields a lift of $P$ and $Q$ to $E/\mathbf{F}_{5^{48}}$, and also of $e_1$ and $e_2$ to $E/\mathbf{F}_{5^{48}}$. We will denote the lifts of $e_1$ and $e_2$ to $E/\mathbf{F}_{5^{4}8}$ also by $e_1$ and $e_2$ respectively. Generators of $E/\mathbf{F}_{5^{48}}$ of order 2124864 and 1671972266837078019879428160 respectively are given by

$$\begin{aligned}
R = (&3\cdot s^{47} + 3\cdot s^{46} + 2\cdot s^{45} + 2\cdot s^{44} + 2\cdot s^{43} + 4\cdot s^{40} + 3\cdot s^{39} + s^{38} +\\
&3\cdot s^{37} + s^{36} + 4\cdot s^{35} + s^{34} + 3\cdot s^{33} + 3\cdot s^{31} + 3\cdot s^{30} + 4\cdot s^{29} +\\
&3\cdot s^{25} + 4\cdot s^{24} + 4\cdot s^{23} + 4\cdot s^{22} + 4\cdot s^{20} + 2\cdot s^{19} + 3\cdot s^{18} + 2\cdot s^{17} +\\
&3\cdot s^{16} + 3\cdot s^{15} + 4\cdot s^{13} + 2\cdot s^{11} + 3\cdot s^{10} + s^{9} + 3\cdot s^{8} + s^{6} + s^{5} +\\
&4\cdot s^{4} + s^{3} + 4\cdot s^{2} + 4\cdot s + 4, 3\cdot s^{47} + s^{46} + s^{44} + 4\cdot s^{43} + s^{41} +\\
&s^{40} + 2\cdot s^{39} + 2\cdot s^{37} + 2\cdot s^{35} + s^{34} + 2\cdot s^{33} + 3\cdot s^{32} + s^{31} + 3\cdot s^{30}\\
&+ 3\cdot s^{29} + 3\cdot s^{26} + s^{25} + 2\cdot s^{24} + 3\cdot s^{23} + s^{22} + 2\cdot s^{21} + 3\cdot s^{20} +\\
&2\cdot s^{19} + 4\cdot s^{18} + 3\cdot s^{17} + 3\cdot s^{16} + 2\cdot s^{15} + 3\cdot s^{13} + 2\cdot s^{12} + 4\cdot s^{11} +\\
&s^{10} + 4\cdot s^{9} + s^{8} + 2\cdot s^{7} + s^{6} + 4\cdot s^{5} + 3\cdot s^{4} + 4\cdot s^{3} + 2\cdot s + 3)\\
S = (&2\cdot s^{46} + 4\cdot s^{45} + 4\cdot s^{44} + 4\cdot s^{43} + 4\cdot s^{42} + 2\cdot s^{41} + 2\cdot s^{40} + 4\cdot s^{39} +\\
&s^{38} + 4\cdot s^{37} + 4\cdot s^{36} + 4\cdot s^{33} + s^{32} + 3\cdot s^{31} + 4\cdot s^{30} + 4\cdot s^{29} + s^{28}\\
&+ s^{26} + 4\cdot s^{23} + 4\cdot s^{22} + 3\cdot s^{18} + s^{17} + 3\cdot s^{16} + 4\cdot s^{15} + 4\cdot s^{13} +\\
&3\cdot s^{12} + 4\cdot s^{10} + s^{9} + 3\cdot s^{7} + s^{6} + s^{5} + 4\cdot s^{4} + 3\cdot s^{3} + 4\cdot s^{2} + 2\cdot s\\
&+ 1 : s^{47} + 3\cdot s^{46} + 2\cdot s^{45} + 4\cdot s^{44} + s^{43} + 4\cdot s^{42} + 3\cdot s^{41} + 4\cdot s^{40}\\
&+ 4\cdot s^{39} + s^{38} + 4\cdot s^{37} + 4\cdot s^{36} + 2\cdot s^{35} + s^{34} + s^{33} + s^{32} + 4\cdot s^{31}\\
&+ 3\cdot s^{30} + s^{28} + s^{27} + 4\cdot s^{25} + 3\cdot s^{24} + 3\cdot s^{23} + 2\cdot s^{22} + 4\cdot s^{20} +\\
&3\cdot s^{19} + s^{18} + 3\cdot s^{17} + 3\cdot s^{16} + 2\cdot s^{15} + s^{14} + 4\cdot s^{13} + 3\cdot s^{12} +\\
&4\cdot s^{11} + s^{10} + 3\cdot s^{9} + 4\cdot s^{8} + 2\cdot s^{7} + 4\cdot s^{6} + 2\cdot s^{5} + 4\cdot s^{4} + 2\cdot s^{3} +\\
&2\cdot s^{2} + s + 4)
\end{aligned}$$

Multiplying $R$ and $S$ by all the prime factors of their respective orders not equal to 2 will then give two generators of $E[64]$:

$$\begin{aligned} f_1 &= [3^2 \cdot 7 \cdot 17 \cdot 31]R \\ f_2 &= [5 \cdot 7 \cdot 17 \cdot 31 \cdot 73 \cdot 229 \cdot 5953 \cdot 6673 \cdot 10321 \cdot 22961]S \end{aligned}$$

However, we do not necessarily have that these get mapped to (the lifts of) the generators $e_1, e_2$ of $E[32]$. Indeed they don't. Therefore we apply the change of coordinates

$$\begin{aligned} f_1' &= 12 \cdot f_1' + 15 \cdot f_2' \\ f_2' &= 11 \cdot f_1' + 6 \cdot f_2' \end{aligned}$$

These are still points of order 64, they are independent, and moreover:

$$\begin{aligned} [2]f_1' &= e_1 \\ [2]f_2' &= e_2 \end{aligned}$$

A calculation shows that the Frobenius automorphism $\varphi\colon E[64] \to E[64]$ has the following effect on these generators:

$$\begin{aligned} \varphi(f_1') &= 17f_1' + 3f_2', \\ \varphi(f_2') &= 3f_1' + 46'f_2', \end{aligned}$$

hence $\varphi$ has matrix

$$M_{\varphi,64} = \begin{pmatrix} 17 & 3 \\ 3 & 46 \end{pmatrix}.$$

Note that the trace is $63 \equiv 7 \pmod{64}$ and furthermore that

$$M_{\varphi,64} \equiv M_{\varphi,32} \pmod{32}$$

where the modulus is taken entry-wise. Hence everything works out rather nicely.

We compute one more example, but this time by computing $E[191]$ in the curve $E/\mathbf{F}_{5^{19}}$. Represent $\mathbf{F}_{5^{19}}$ as $F_5(s)$ with

$$s^{19} + s^3 + 2s + 3 = 0.$$

As an abelian group, $E/\mathbf{F}_{5^{19}}$ is isomorphic to $\mathbf{Z}/191\mathbf{Z} \oplus \mathbf{Z}/99861226577\mathbf{Z}$, with generators

$$\begin{aligned}R = (&3s^{17} + 3s^{16} + 2s^{15} + 4s^{14} + 2s^{13} + 4s^{10} \\ &+ 2s^8 + 3s^6 + s^5 + s^4 + s^3 + 4s + 3, \\ &4s^{18} + 2s^{17} + 3s^{15} + 2s^{14} + 2s^{13} + 4s^{12} + 4s^{11} \\ &+ 2s^{10} + 3s^8 + 3s^7 + s^6 + 4s^5 + 4s^4 + 4s^2), \\ S = (&4s^{16} + 4s^{15} + 2s^{12} + s^{11} + 4s^{10} + s^9 + 2s^8 + 2s^7 + s^6 \\ &+ 4s^5 + 3s^4 + s^3 + 4s^2 + 2s, \\ &3s^{18} + 4s^{17} + 2s^{16} + 4s^{15} \\ &+ 2s^{14} + 4s^{13} + 2s^{10} + 3s^9 \\ &+ 3s^8 + s^6 + 2s^5 + 3s^4 + 3s^3 \\ &+ 4s^2 + 2)\end{aligned}$$

of order $191 = 191$ and $99861226577 = 7 \cdot 191 \cdot 419 \cdot 178259$ respectively. Hence

$$\begin{aligned}f_1 &= R \\ f_2 &= [7 \cdot 419 \cdot 178259]S\end{aligned}$$

are two distinct elements of order 191, hence they generate $E[191] = \langle f_1, f_2 \rangle$ as $\mathbf{Z}/191\mathbf{Z}$-modules. Applying the Frobenius map $\varphi\colon E[191] \to E[191]$ yields

$$\begin{aligned}\varphi(f_1) &= 189 f_1 + 188 f_2, \\ \varphi(f_2) &= 66 f_1 + 1 f_2.\end{aligned}$$

Therefore $\varphi\colon E[191] \to E[191]$ has matrix

$$\begin{pmatrix} 189 & 66 \\ 188 & 1 \end{pmatrix}$$

with respect to the basis $f_1, f_2$. This matrix has trace $190 \pmod{191}$. According to our formula, this implies

$$\begin{aligned}\#E(\mathbf{F}_5) &= 1 + 5 - \mathrm{Tr}(\varphi_{191}) \\ &\equiv -184 \pmod{191} \\ &\equiv 7 \pmod{191},\end{aligned}$$

and since $0 \leq \#E(\mathbf{F}_5) \leq 25$, we have again $\#E(\mathbf{F}_5) = 7$.

# Part III

# Serre's $N_X(p)$ theorem for elliptic curves

# Chapter 8

# Proof of Serre's $N_X(p)$ theorem for elliptic curves

We state and give the proof of theorem 8.1 from Serre [12] in the case of elliptic curves.

**Theorem 8.1** *Let $E$, $E'$ be two elliptic curves over $\mathbf{Q}$, such that $N_E(p) = N_{E'}(p)$ for a set primes of (Dirichlet or natural) density 1. Then $N_E(p^e) = N_{E'}(p^e)$ for all $p$ where both $E$ and $E'$ have good reduction, and all $e \geq 1$.*

**Remark 8.2** The theorem holds both for the Dirichlet density and the natural density because in the proof Chebotarev's density theorem is invoked. Chebotarev's density theorem also holds for both densities.

**Remark 8.3** It suffices to show that $N_E(p) = N_{E'}(p)$ for all primes where $E$ and $E'$ have good reduction, because the remainder of the theorem then immediately follows from remark 7.4.

For a number field $K$ we denote the set of places of $K$ by $V_K$.

For a prime $\mathfrak{p}$ of $K$ we denote the local field of $K$ at $\mathfrak{p}$ by $K_{\mathfrak{p}}$.

For a local field $K$ we denote its ring of integers by $\mathcal{O}_K$, and a uniformiser for its unique prime ideal by $\pi$.

We will now prove theorem 8.1. To do so we need to extend $\mathbf{Q}$ to a field $K$ so that $E(K)$ contains all the $\ell^m$-torsion, where $\ell$ is prime. We wish to eventually apply Chebotarev's density theorem, hence we must know something about the splitting behaviour of the rational primes of $\mathbf{Q}$ in this extension $K$.

**Proposition 8.4** *Let $E/\mathbf{Q}$ be an elliptic curve, $\ell$ a rational prime, $m$ a positive integer, $\Delta$ the discriminant of $E$, $S_\ell$ the set of rational primes consisting of $\ell$ and the primes that divide $\Delta$. Let $K = \mathbf{Q}(E[\ell^m])$. Then $K$ is unramified outside $S_\ell$.*

Proof This is a direct consequence of part II corollary 6.13. ■

**Remark 8.5** Note that $S_\ell$ depends on $\ell$ but not on the power $m$.

**Definition 8.6** Let $S$ be a finite subset of $V_K$, and let $\Omega$ be a set with the discrete topology. Consider a map $f\colon V_K - S \to \Omega$. We say that $f$ is $S$-*frobenian* if there exists a finite Galois extension $L/K$, unramified outside $S$, and a map $\varphi\colon G \mapsto \Omega$, where $G = \mathrm{Gal}(L/K)$, such that:

a) $\varphi$ is invariant under conjugation (i.e. $\varphi$ factors through $G \mapsto \mathrm{Cl}\, G$, where $\mathrm{Cl}\, G$ denotes the set of conjugacy classes of $G$),

b) $f(v) = \varphi(\sigma_v)$ for all $v \in V_K - S$.

**Definition 8.7** A subset $\Sigma$ of $V_K - S$ is said to be $S$*-frobenian* if its characteristic function is $S$-frobenian. This means that there exists a Galois extension $L/K$ as above, and a subset $C$ of its Galois group $G$, stable under conjugation, such that $v \in \Sigma \iff \sigma_v \in C$.

The coincidence on a set of primes of density 1 implying the coincidence everywhere is based on the Chebotarev density theorem. The main step is the following theorem, which will allow us to apply Chebotarev's density theorem.

**Theorem 8.8** *Let $E/\mathbf{Q}$ be an elliptic curve, $\ell$ a prime and $m \in \mathbf{Z}_{>0}$. Then*

$$V_{\mathbf{Q}} \to \mathbf{Z}/\ell^m\mathbf{Z}\colon p \mapsto N_E(p) \pmod{\ell^m}$$

*is $S_\ell$-Frobenian.*

Proof Recall that $K/\mathbf{Q}$ is a Galois extension such that $E(K)$ contains all the $\ell^m$-torsion. Recall furthermore that $S_\ell$ is the finite set of rational primes consisting of

- $\ell$;
- All the rational primes for which $E$ has bad reduction, that is those primes that divide the discriminant $\Delta$ of $E$.

Let $p \in V_{\mathbf{Q}} - S$ and let $\mathfrak{p}$ be an ideal of $K$ lying over $(p)$. Then $E(K_{\mathfrak{p}})$ is an elliptic curve that also contains all the $\ell^m$ torsion, as $K \subset K_{\mathfrak{p}}$. By Silverman and Tate [15] proposition VII.3.1 (b), the map

$$E(K)[\ell^m] \to \tilde{E}(\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}})$$

is injective. Here the tilde means reduction modulo $\mathfrak{p}$.

To show that $N_E(p) \pmod{\ell^m}$ is $S$-Frobenian we need to find a map

$$\varphi\colon\ \mathrm{Gal}(K/\mathbf{Q}) \to \mathbf{Z}/\ell^m\mathbf{Z}$$

such that

- $\varphi$ is invariant under conjugation (i.e. constant on conjugacy classes of $\mathrm{Gal}(K/\mathbf{Q})$);

- $N_E(p) \pmod{\ell^m} = \varphi(\sigma_p)$ for all $p \in V_{\mathbf{Q}} - S$, where $\sigma_p$ is the conjugacy class of the Frobenius element of the decomposition group $D_{\mathfrak{p}}$. This is well defined since $(p)$ is unramified, and $\varphi$ is constant on conjugacy classes.

We define the map $\varphi$ as follows:

$$\begin{aligned}\varphi\colon\ &\mathrm{Gal}(K/\mathbf{Q}) \to \mathbf{Z}/\ell^m\mathbf{Z}\\ &\qquad\qquad \tau \mapsto 1 - \mathrm{Tr}(\tau \,|\, E(K)[\ell^m]) + \mathrm{Det}(\tau \,|\, E(K)[\ell^m]) \pmod{\ell^m},\end{aligned}$$

Note that $\varphi$ is indeed constant on conjugacy classes, since the trace and determinant are similarity invariant.

What is left to show is that $N_E(p) \pmod{\ell^m}$ is equal to the composition $p \mapsto \sigma_p \mapsto \varphi(\sigma_p)$. For this, note that $K_{\mathfrak{p}}/\mathbf{Q}_p$ is a Galois extension with Galois group $D_{\mathfrak{p}}$, which is generated by any element of the conjugacy class $\sigma_p$. This means that any element of $\sigma_p$ in fact also acts on $E(K_{\mathfrak{p}})$. Hence we can also compute $\mathrm{Tr}(\sigma_p \,|\, E(K_{\mathfrak{p}})[\ell^m])$. But since $K \subset K_{\mathfrak{p}}$ and in fact all the $\ell^m$-torsion is already in $K$, we have

$$\begin{aligned}\mathrm{Tr}(\sigma_p \,|\, E(K_{\mathfrak{p}})[\ell^m]) &= \mathrm{Tr}(\sigma_p \,|\, E(K)[\ell^m]) \pmod{\ell^m},\\ \mathrm{Det}(\sigma_p \,|\, E(K_{\mathfrak{p}})[\ell^m]) &= \mathrm{Det}(\sigma_p \,|\, E(K)[\ell^m]) \pmod{\ell^m}.\end{aligned}$$

We can take this one step further, by using that the reduction modulo $\mathfrak{p}$ induces an injection

$$E(K_{\mathfrak{p}})[\ell^m] \hookrightarrow \tilde{E}(\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}}).$$

This implies that the reduction map gives an isomorphism

$$E(K_{\mathfrak{p}})[\ell^m] \xrightarrow{\sim} \tilde{E}(\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}})[\ell^m]$$

of $\mathbf{Z}/\ell^m\mathbf{Z}$-modules. Now the reduction map consists of multiplying a point on $E(K_{\mathfrak{p}})$ with projective coordinates $[x_0, y_0, z_0]$, with a suitable power of $\pi$ such that all the coordinates become elements of $\mathcal{O}_{K_{\mathfrak{p}}}$ and at least one becomes an element of $\mathcal{O}^*_{K_{\mathfrak{p}}}$, and then taking everything $\pmod{\mathfrak{p}}$. Note that under the above isomorphism, the action of $\sigma_p$ on $E(K_{\mathfrak{p}})[\ell^m]$ becomes an action on $\tilde{E}(\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}})[\ell^m]$ which on coordinates of points is given by $x \mapsto x^p \pmod{\mathfrak{p}}$. Hence we see that

$$\begin{aligned}\mathrm{Tr}(\sigma_p \,|\, E(K_{\mathfrak{p}})[\ell^m]) &= \mathrm{Tr}(x \mapsto x^p \,|\, \tilde{E}(\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}})[\ell^m]) \pmod{\ell^m},\\ \mathrm{Det}(\sigma_p \,|\, E(K_{\mathfrak{p}})[\ell^m]) &= \mathrm{Det}(x \mapsto x^p \,|\, \tilde{E}(\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}})[\ell^m]) \pmod{\ell^m}.\end{aligned}$$

In the proof of Silverman [14, theorem V.2.3.1] we see that the above determinant is equal to $p$ and the trace is equal to $1 + p - \#E(\mathbf{F}_p)$. Hence

$$\begin{aligned}\varphi(\sigma_p) &= 1 - \mathrm{Tr}(x \mapsto x^p \mid \tilde{E}(\mathcal{O}_{K_\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})[\ell^m]) \\ &\quad + \mathrm{Det}(x \mapsto x^p \mid \tilde{E}(\mathcal{O}_{K_\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})[\ell^m]) \pmod{\ell^m} \\ &= 1 - \mathrm{Tr}(x \mapsto x^p \mid \tilde{E}(\mathcal{O}_{K_\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})[\ell^m]) + p \pmod{\ell^m} \\ &= \#\tilde{E}(\mathbf{F}_p) \pmod{\ell^m} \\ &= N_E(p) \pmod{\ell^m}\end{aligned}$$ ■

Note that if a function $f\colon V_K - S \to \Omega$ is $S$-frobenian and $S \subset T \subset V_K$, then $f\colon V_K - T \to \Omega$ is also $T$-frobenian. Hence we have the following corollary.

**Corollary 8.9** *Let $E, E'$ be two elliptic curves over $\mathbf{Q}$. Let $\ell$ be a rational prime, $m$ a positive integer. Let $S_\ell$ and $S'_\ell$ be as in the previous lemma corresponding to $E$ and $E'$ respectively. Then $N_E(p)\colon V_\mathbf{Q} - S_\ell \cup S'_\ell \to \mathbf{Z}/\ell^m\mathbf{Z}$ and $N_{E'}(p)\colon V_\mathbf{Q} - S_\ell \cup S'_\ell \to \mathbf{Z}/\ell^m\mathbf{Z}$ are $S_\ell \cup S'_\ell$-frobenian.*

Proof Note that $S_\ell, S'_\ell \subset S_\ell \cup S'_\ell$. ■

**Remark 8.10** Consider the setting of definition 8.7 of $S$-frobenian sets. Chebotarev's density theorem shows that $\Sigma$ has a density, which is equal to $\#C/\#G$.

We wish to apply this to fibers of frobenian functions. We have the following

**Lemma 8.11** *Let $f\colon V_K - S \to \Omega$ be an $S$-frobenian function, $L/K$ be a corresponding finite Galois extension unramified outside $S$. Let $W \subset \Omega$. Then the pre-image $f^{-1}(W)$ is a $S$-frobenian set.*

Proof Note that

$$\begin{aligned}f^{-1}(W) &= \{v \in V_K - S : \varphi(\sigma_v) \in W\} \\ &= \{v \in V_K - S : \sigma_v \in \varphi^{-1}(W)\},\end{aligned}$$

and note that $\varphi^{-1}(W)$ is a union of conjugacy classes, since $\varphi$ is constant on conjugacy classes. Hence $v \in f^{-1}(W)$ if and only if $\sigma_v \in \varphi^{-1}(W)$, hence $f^{-1}(W)$ is $S$-frobenian. ■

**Lemma 8.12** *Let $f, f'\colon V_K - S \to \Omega$, be two $S$-frobenian functions. Then $(f, f')\colon V_K - S \to \Omega \times \Omega$ is $S$-frobenian.*

Proof Let finite Galois extensions $L, L'/K$, Galois groups $G, G'$ and maps $\varphi, \varphi'\colon G \to \Omega$ correspond to $f, f'$ respectively. Then the compositum $LL'$ is Galois over $K$, and $LL'$ is unramified outside $S$. Furthermore, we have the embedding $\mathrm{Gal}(LL'/K) \hookrightarrow \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K)$. We can compose this with the map $\mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K) \to \Omega \times \Omega\colon (\sigma, \sigma') \mapsto (\varphi(\sigma), \varphi'(\sigma'))$. Let $v$ be a place of $K$, $w|v$ be a place of $L$ and $u|w$ a place of $LL'$. Note that the map $\mathrm{Gal}(LL'/K) \to \mathrm{Gal}(L/K)$ sends a generator of $D_{(u,v)}$ to a generator of $D_{(w,v)}$, for the generators are characterised by $x \mapsto x^{\mathbf{N}\mathfrak{p}_v}$ on the residue field. Hence $\sigma_{(u,v)}$ gets mapped to $\sigma_{(w,v)}$. This shows that the previous composition is equal to $(f, f')$, hence that $(f, f')$ is frobenian. ■

We are now ready to prove theorem 8.1.

**Theorem (see theorem 8.1)** *Let $E$ and $E'$ be elliptic curves over $\mathbf{Q}$. Suppose that $N_E(p) = N_{E'}(p)$ for a set of primes of density 1. Then in fact $N_E(p^e) = N_{E'}(p^e)$ for all $e \geq 1$ and all primes $p$ where both $E$ and $E'$ have good reduction.*

Proof Let $\ell$ be a prime, $m$ be a positive integer. Let $S_\ell, S'_\ell$ be the sets corresponding to $E, E'$ from theorem 8.8. Let $S = S_\ell \cup S'_\ell$. That is, $S$ consists of the rational primes that divide $\ell\Delta\Delta'$ with $\Delta, \Delta'$ the discriminants of $E, E'$ respectively. By theorem 8.8 and corollary 8.9 $N_E \pmod{\ell^m}$ and $N_{E'} \pmod{\ell^m}$ are $S$-frobenian. By lemma 8.12 the map $(N_E \pmod{\ell^m}, N_{E'} \pmod{\ell^m}) : V_{\mathbf{Q}} - S \to \mathbf{Z}/\ell^m\mathbf{Z} \times \mathbf{Z}/\ell^m\mathbf{Z}$ is $S$-frobenian. Let $D$ be the diagonal in $\Omega \times \Omega$ By lemma 8.11 the inverse image of the complement of the diagonal

$$(N_E, N_{E'})^{-1}(\Omega \times \Omega - D) = \{p \in V_{\mathbf{Q}} - S : N_E(p) \neq N_{E'}(p) \pmod{\ell^m}\}$$

is a frobenian set. But since its density is zero it must be empty, by Chebotarev's density theorem. Hence $N_E(p) = N_{E'}(p) \pmod{\ell^m}$ for all $p \in V_{\mathbf{Q}} - S$ and positive integers $m$. Note that $S$ did not depend on $m$. By taking $m$ large enough we conclude that $N_E(p) = N_{E'}(p)$ for all $p \in V_{\mathbf{Q}} - S$. We can repeat the entire argument with a prime different from $\ell$ to conclude that also $N_E(\ell) = N_{E'}(\ell)$, except if $E$ or $E'$ has bad reduction at $\ell$. To obtain the equality $N_E(p^e) = N_{E'}(p^e)$ apply remark 7.4. This finishes the proof. ■

**Remark 8.13** The result (for elliptic curves) is also stated in the first proposition of section 2.3 in Serre [10].

## 8.1 Application to modular forms

We will not explain what modular forms are, but we will state a corollary of theorem 8.1 about modular forms.

**Corollary 8.14** *Let $f$ and $f'$ denote two newforms of weight two for $\Gamma_0(N)$. Assume that $f$ and $f'$ are normalized so that their first order Fourier coefficients are one, and suppose that all coefficients are in $\mathbf{Z}$. If for a set of primes $p$ of density 1 the Fourier coefficients $a_p(f) = a_p(f')$ are equal, then they are equal for all primes not dividing $N$.*

Proof By Eichler-Shimura theory (see, e.g., Knapp [6, theorem 11.74 and theorem 12.8]), there exists two elliptic curves $E$ and $E'$ of conductor $N$ such that $a_p(f) = a_p(E)$ and $a_p(f') = a_p(E')$, where $a_p(E) = N_E(p)$. Now the result follows from theorem 8.1.

# Acknowledgements

I would like to thank my supervisor, Gunther Cornelissen, for all the advice and guidance he provided while I was working on this thesis, and for the stimulating enthousiasm during our meetings.

I would also like to thank Valentijn Karemaker for telling me about the proof she knew of Chebotarev's density theorem and helping me understand it.

# Bibliography

[1] Henri Cohen. *Number Theory: Volume I: Tools and Diophantine Equations*, volume 239 of *Graduate Texts in Mathematics*. Springer-Verlag, 2007. ISBN 978-0-387-49922-2.

[2] R. Descombes. *Éléments de théorie des nombres*. Presses universitaires de France, 1986.

[3] Vladimir Dokchitser. Algebraic number theory lecture notes.

[4] Michael D. Fried and Moshe Jarden. *Field Arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, 1986. ISBN 978-3-662-07218-9.

[5] Larry Joel Goldstein. *Analytic Number Theory*. Prentice-Hall, Englewood Cliffs, New Jersey, 1971. ISBN 9780130348432.

[6] Anthony W. Knapp. *Elliptic Curves*. Mathematical Notes - Princeton University Press. Princeton University Press, 1992. ISBN 9780691085593.

[7] Anthony W. Knapp. *Advanced Algebra*. Cornerstones. Birkhaüser, 2007.

[8] Serge Lang. *Algebra*. Addison-Wesley World Student Series. Addison-Wesley, 1965.

[9] Serge Lang. *Algebraic Number Theory*. Addison-Wesley Series in Mathematics. Addison-Wesley, 1970.

[10] Jean-Pierre Serre. *Abelian $l$-adic representations and elliptic curves*. W. A. Benjamin, New York, New York 10016, 1968.

[11] Jean-Pierre Serre. *Linear Representations of Finite Groups*, volume 42 of *Graduate Texts in Mathematics*. Springer-Verlag, 1977. ISBN 0-387-90190-6.

[12] Jean-Pierre Serre. *Lectures on $N_X(p)$*, volume 11 of *Chapman & Hall/CRC Research Notes in Mathematics*. CRC Press, Boca Raton, FL, 2012. ISBN 978-1-4665-0192-8.

[13] David Sheppard and Brian Osserman. Rings of integers and ideal class groups, 2000. URL `https://www.math.ucdavis.edu/~osserman/seminar/`.

[14] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. ISBN 978-0-387-09493-9.

[15] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992. ISBN 0-387-97825-9.

# Index