Lecture Notes in Mathematics

Editors: J.-M. Morel, Cachan F. Takens, Groningen B. Teissier, Paris

Springer Berlin

Berun Heidelberg New York Barcelona Hong Kong London Milan Paris Singapore Tokyo **Clemens Adelmann**

The Decomposition of Primes in Torsion Point Fields



Author

Clemens Adelmann Technical University Braunschweig Institute of Applied Mathematics Dept. of Applied Algebra Pockelsstr.14 38106 Braunschweig, Germany

E-mail: c.adelmann@tu-bs.de

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Adelmann, Clemens: The decomposition of primes in torsion point fields / Clemens Adelmann. - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2001 (Lecture notes in mathematics ; 1761) ISBN 3-540-42035-5

Mathematics Subject Classification (2000): 11-02, 11R21, 11R32, 11R09, 11G05, 11F11, 13A50, 12Y05

ISSN 0075-8434 ISBN 3-540-42035-5 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

© Springer-Verlag Berlin Heidelberg 2001 Printed in Germany

Typesetting: Camera-ready $T_E X$ output by the author SPIN: 10836966 41/3142-543210 - Printed on acid-free paper

Table of Contents

1	Inti	roduction	1		
2	Decomposition Laws				
	2.1	Foundations of Prime Ideal Decomposition	5		
	2.2	Decomposition in Abelian Extensions	11		
	2.3	Density Statements	22		
3	Elliptic Curves				
	3.1	Defining Equations	25		
	3.2	Addition on Elliptic Curves	26		
	3.3	Division Polynomials	28		
	3.4	Torsion Points	30		
	3.5	ℓ -adic Representations	32		
	3.6	Reduction Modulo ${\mathfrak p}$ and L-Series	35		
4	Elli	ptic Modular Curves	41		
	4.1	Modular Curves	41		
	4.2	Modular Forms	45		
	4.3	Hecke Operators	48		
	4.4	The Eichler-Shimura Formula	54		
5	Tor	sion Point Fields	59		
	5.1	The Groups $GL(2,n)$	59		
	5.2	Subfields of $k(E_n)$	66		
	5.3	Defining Polynomials of Subfields of $k(E_n)$	73		
	5.4	Decomposition in 2- and 3-Torsion Point Fields	76		
	5.5	Decomposition in 4-Torsion Point Fields	80		
	5.6	Decomposition in p^m -Torsion Point Fields	85		
6	Invariants and Resolvent Polynomials				
	6.1	Foundations of Galois Theory	87		
	6.2	Procedure for the Description of Subfields	90		
	6.3	Invariant Algebras	91		
	6.4	Application to 4-Torsion Point Fields	100		

Appendices				
Α	Invariants of Elliptic Modular Curves 109			
в	L-series Coefficients a_p			
\mathbf{C}	Fully Decomposed Prime Numbers 119			
D	Resolvent Polynomials 127			
\mathbf{E}	Free Resolution of the Invariant Algebra			
References				
References				
Symbols				

1 Introduction

It is an historical goal of algebraic number theory to relate all algebraic extensions of a number field in a unique way to structures that are exclusively described in terms of the base field. Suitable structures are the prime ideals of the ring of integers of the considered number field. By examining the behaviour of the prime ideals when embedded in the extension field, sufficient information should be collected to distinguish the given extension from all other possible extension fields.

The ring of integers \mathcal{O}_k of an algebraic number field k is a Dedekind ring. Any non-zero ideal in \mathcal{O}_k possesses therefore a decomposition into a product of prime ideals in \mathcal{O}_k which is unique up to permutations of the factors. This decomposition generalizes the prime factor decomposition of numbers in \mathbb{Z} . In order to keep the uniqueness of the factors, view has to be changed from elements of \mathcal{O}_k to ideals of \mathcal{O}_k .

Given an extension K/k of algebraic number fields and a prime ideal \mathfrak{p} of \mathcal{O}_k , the decomposition law of K/k describes the product decomposition of the ideal generated by \mathfrak{p} in \mathcal{O}_K and names its characteristic quantities, i. e. the number of different prime ideal factors, their respective inertial degrees, and their respective ramification indices.

When looking at decomposition laws, we should initially restrict ourselves to Galois extensions. This special case already offers quite a few difficulties. Besides, any extension of number fields is a subfield of some Galois extension whose decomposition law enables us to draw conclusions on the prime ideal decomposition in the original subextension. On the other hand, restricting the attention to Galois extensions leads to decisive advantages due to the additional structure:

- The decomposition law becomes more simple because all of the appearing ramification indices coincide, as well as all of the inertial degrees.
- The extension is uniquely determined by the decomposition law.

In order to unambiguously identify a given Galois extension, it is not necessary to know the decomposition law in its full generality. Is is enough to determine the set of fully decomposed prime ideals.

It is known how a given prime ideal decomposes in extensions with an abelian Galois group. The classical version of class field theory provides a unique characterization of any abelian extension of a number field k by means of ideal groups in k from which the respective Galois group and the decomposition law may be read off.

The results and methods of class field theory are restricted to abelian extensions because they rely on the multiplicative structure of the base field. So, if we intend to describe non-abelian extensions, we have to look for appropriate structures which abstract from the abelian nature of ideal groups.

Some attempts in this direction start as follows:

- We neglect the multiplicative structure and investigate sets of prime ideals in order to distinguish between the extensions.
- Any extension K/k can be described by a polynomial which is the minimal polynomial of some primitive element of \mathcal{O}_K . If K/k is a Galois extension, we may use instead a polynomial whose splitting field is equal to K. In this case, the decomposition of a prime ideal \mathfrak{p} of \mathcal{O}_k is related to the decomposition of the polynomial over the residue field of \mathfrak{p} .

For different reasons, these approaches did not lead to a satisfactory result. We content ourselves therefore with analyzing particular extensions which come with additional structures in order to get examples and hints to a more general decomposition law.

The extensions which are examined within these notes are formed by adjunction of the coordinates of torsion points of an elliptic curve. The construction of these extensions runs completely analoguously to forming cyclotomic fields, which are generated by the adjunction of roots of unity, i. e. by the coordinates of certain torsion points of the affine curve defined by the equation $x^2 + y^2 = 1$. Cyclotomic and torsion point extensions both result from the existence of a binary operation on the points of the respective curve. Both types of extensions are Galois because the operation can be described in either case by algebraic equations with coefficients taken from the base field. In the case of the unit circle given by $x^2 + y^2 = 1$, the operation can be interpreted as multiplication in \mathbb{C} .

In contrast to cyclotomic fields, the examined torsion points fields are nonabelian, even non-solvable extensions, if we disregard few simple exceptional cases. The methods of class field theory therefore only provide partial results. On the other hand, the close connection to geometric objects supplies the following data on torsion point fields:

- We are able to derive a defining polynomial from the formulas of the composition law of the points on the elliptic curve.
- The elements of the Galois group can be interpreted as 2×2 -matrices due to the structure of the set of torsion points. In this way, we get a concrete description of the Galois operation on the field elements and severe restrictions to the shape of the Galois group.

- The coefficients of the L-series of the elliptic curve appear in different contexts. They supply additional arithmetic quantities which may be used for the characterization of the extension.

Two further restrictions ease the investigations and simplify the formulations without losing too much of the deep interconnections:

- Choosing the elliptic modular curves $X_0(N)$ offers the opportunity that their L-series coefficients with prime number index p coincide with the eigenvalues of the corresponding p-th Hecke operators. However, at most finitely many exceptional p may have to be excluded or treated separately.
- It suffices to examine the torsion points of prime power order to cover the case of a general fixed order.

If we only use L-series coefficients and results from subfields which are abelian or Kummer extensions then we will get the complete decomposition law only in the cases $p^m = 2$ [Ito82] and $p^m = 3$ [Renn89]. This fact was already observed by Shimura who analyzed *p*-torsion point extensions for $X_0(11)$ and certain prime numbers *p* in [Shim66].

For this reason, we also pursue the approach to the decomposition law by means of defining polynomials. The degree of the appearing polynomials is quite high, but we can reduce the investigation to subfields which can be described by polynomials with lower degree at the cost of possibly larger coefficients. The combined use of the described procedures should lead to efficiently evaluable formulations of the decomposition law in torsion point extensions.

The previous elucidations demonstrate the leitmotif of the present notes. They include revised data and results from a DFG research report [Adel94], the dissertation [Adel96] and the work-out of some seminar lectures.

At first, we describe the general formulation of a decomposition law. Then we present commonly known results of class field theory which serve as a basis for the conclusions we will draw from abelian and Kummer subextensions. The chapter terminates with results on general Galois extensions using different notions of density which culminate in the Theorems of Chebotarev and Bauer.

The following chapter recalls basic facts on elliptic curves which will be used within these notes. In particular, division polynomials and L-series are introduced which provide characteristic quantities for the extensions to be investigated.

A succinct glance into the theory of modular curves describes the notions of modular forms and Hecke operators defined on them. The survey ends up in the Eichler-Shimura formula which provides an intimate link between the coefficients of the L-series of an elliptic modular curve and the Fourier coefficients of a cusp form which is an eigenform of all Hecke operators. This formula is at our disposal when we take a closer look at the torsion point extensions.

We start our investigations by listing the properties of torsion point fields. Using the ℓ -adic representations we show that their Galois groups are matrix groups of the form GL(2, n). These groups are examined in greater detail. We mention important normal subgroups which correspond to Galois subfields of the *n*-torsion point field. Using these subfields, our consideration can be performed step by step in appropriate partial extensions. In this way, the decomposition behaviour of prime ideals in general torsion point extensions is reduced to the cases of torsion points of prime number order p and the transition from p^m to p^{m+1} .

Using the results obtained so far, we give criteria describing the decomposition in p^m -torsion point extensions. The differing special cases $p^m = 2, 3, 4$ are treated separately in more detail.

Within our decomposition statements, some defining polynomials of Galois subfields contribute to the classification. In Chapter 6 we give the general procedure which is the basis for the calculation of the wanted defining polynomial. This description is preceded by recalling the used basic facts of invariant theory. The general method is then applied to a particular subfield of the 4-torsion point field which appeared before, and a defining polynomial is calculated for this field.

In the appendix, we collect some numerical data that we calculated in connection with the decomposition law. It contains characteristic quantities of the elliptic modular curves, the first coefficients of their L-series, fully decomposed prime numbers in some selected torsion point extensions below a given bound, certain resolvent polynomials, and the free resolution of an invariant algebra.

I would like to thank H. Opolka for his generous assistance. His comments were a valuable help to me in writing these notes.

2 Decomposition Laws

In this chapter we describe the properties and the significance of decomposition laws in extensions of algebraic number fields. In this way we settle a basis for the formulation of these laws, and we mention results from abelian and Kummer extensions which offer important contributions to the investigations below.

In the first section we define basic notions and name characteristic quantities appearing in connection with decomposition laws. We explain how the decomposition of a prime ideal can be obtained by using the product decomposition of a polynomial into irreducible factors (Theorem 2.1.1) and how the decomposition behaviour in general extensions can be read off from suited Galois extensions (Theorem 2.1.2). We emphasize the simplification of the decomposition law in the case of Galois extensions.

The second section is restricted to abelian extensions. After introducing the important notions of class field theory in the ideal theoretic language of [Hass67], we characterize all abelian extensions of a given number field by ideal groups and the Artin map. Then we formulate the decomposition law for general abelian extensions (Theorem 2.2.4) and especially for cyclic Kummer extensions (Theorem 2.2.5) as well as cyclotomic extensions of \mathbb{Q} (Theorem 2.2.6).

In Section 2.3, we introduce the notion of Dirichlet density of prime ideal sets. From the Theorems of Chebotarev (Theorem 2.3.1) and Bauer (Theorem 2.3.2) we conclude that a Galois extension is uniquely determined by its set of fully decomposed prime ideals.

2.1 Foundations of Prime Ideal Decomposition

Quite a few of the statements given below can be considered as basic facts of algebraic number theory. Their proofs as well as a more detailed account to them may be found in [Janu73] or in [Neuk92].

Let k be an algebraic number field (with $[k : \mathbb{Q}] < \infty$). Consider the set of elements of k whose (normalized) minimal polynomials over \mathbb{Q} possess integral coefficients. They form a subring of k called ring of integers \mathcal{O}_k . In \mathcal{O}_k each prime ideal \mathfrak{p} different from $\{0\}$ is maximal, and the quotient $\kappa(\mathfrak{p}) = \mathcal{O}_k/\mathfrak{p}$ is a finite field called the residue field belonging to \mathfrak{p} . If we define the multiplication of ideals by $\mathfrak{a}b = \{\sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$ then any ideal of k, i. e. any ideal of \mathcal{O}_k different from $\{0\}$, has a decomposition into a finite product of prime ideals of k which is unique up to permutations of the factors.

Let K/k be a finite extension of algebraic number fields and \mathfrak{p} a prime ideal of k. If \mathfrak{P} is a prime ideal of K lying over \mathfrak{p} , i. e. satisfying $\mathfrak{P} \cap \mathcal{O}_k = \mathfrak{p}$, the residue field $\kappa(\mathfrak{P})$ is a finite extension of $\kappa(\mathfrak{p})$.

The prime ideal \mathfrak{p} maps by the rule $\mathfrak{p} \mapsto \mathfrak{p}\mathcal{O}_K$ to an ideal of the ring of integers \mathcal{O}_K which is called the ideal generated by \mathfrak{p} in \mathcal{O}_K . $\mathfrak{p}\mathcal{O}_K$ is not prime in general, but in \mathcal{O}_K it owns a product decomposition

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_q^{e_g}, \qquad (2.1)$$

where \mathfrak{P}_i is a prime ideal with *inertial degree* f_i over \mathfrak{p} , and the prime ideals \mathfrak{P}_i are distinct. The exponent e_i of \mathfrak{P}_i is called the *ramification index* of \mathfrak{P}_i over \mathfrak{p} . The set of prime ideals of K lying over \mathfrak{p} is denoted by $P_{K/k}(\mathfrak{p})$,

$$P_{K/k}(\mathfrak{p}) = \{ \mathfrak{P} \mid \mathfrak{P} \text{ prime ideal of } K , \mathfrak{P} \cap \mathcal{O}_k = \mathfrak{p} \} = \{ \mathfrak{P}_1, \dots, \mathfrak{P}_g \}.$$

Inertial degree and ramification index also appear in the following shape:

1. f_i is the degree of the extension of the residue fields belonging to \mathfrak{P}_i and \mathfrak{p} , respectively,

$$f_i = f_{K/k}(\mathfrak{P}_i) = [\kappa(\mathfrak{P}_i) : \kappa(\mathfrak{p})].$$

2. f_i is the exponent of the relative norm of \mathfrak{P}_i belonging to K/k,

$$N_{K/k}(\mathfrak{P}_i) = \mathfrak{p}^{f_i}.$$

3. e_i measures the increase of the value group of the \mathfrak{P}_i -adic continuation $\varphi_{\mathfrak{P}_i}: K \to \mathbb{R}$ of a \mathfrak{p} -adic valuation $\varphi_{\mathfrak{p}}: k \to \mathbb{R}$,

$$e_i = e_{K/k}(\mathfrak{P}_i) = (\varphi_{\mathfrak{P}_i}(K) : \varphi_{\mathfrak{p}}(k))$$
 as index of subgroups of \mathbb{R} .

A prime ideal \mathfrak{p} is called *unramified* with respect to K/k if all exponents e_i in the decomposition (2.1) are equal to 1. If one of the e_i is greater than 1 then \mathfrak{p} is called *ramified*. The prime ideal \mathfrak{p} is *fully decomposed* with respect to K/k if \mathfrak{p} is unramified and all f_i are equal to 1. In this case, $\mathfrak{p}\mathcal{O}_K$ has the maximal possible number of distinct prime ideal factors in \mathcal{O}_K .

The decomposition law of the extension K/k formulates instructions which assign to any prime ideal \mathfrak{p} of k the corresponding decomposition (2.1) of the ideal $\mathfrak{p}\mathcal{O}_K$ generated by \mathfrak{p} in \mathcal{O}_K . The quantities e_i, f_i, g in (2.1) are related by the following formulas.

Proposition 2.1.1.

- (a) Using the terms of (2.1), we have $\sum_{i=1}^{g} e_i f_i = [K:k]$.
- (b) Inertial degree and ramification index are multiplicative: If L/K/k is a chain of extensions and \$\mathcal{P}\$ is a prime ideal of L then we have

$$f_{L/k}(\mathfrak{P}) = f_{L/K}(\mathfrak{P}) \cdot f_{K/k}(\mathfrak{P} \cap \mathcal{O}_K) ,$$

$$e_{L/k}(\mathfrak{P}) = e_{L/K}(\mathfrak{P}) \cdot e_{K/k}(\mathfrak{P} \cap \mathcal{O}_K) .$$

Proof.

(a) see [Neuk92, I. Satz 8.2]. (b) see [Janu73, I §6, p. 26f.]. The assertion results from the multiplicativity of norm and index (cf. 2. and 3. above). \Box

One principal way to find out the decomposition of a prime ideal \mathfrak{p} of k in the extension of number fields K/k of degree n is to use a polynomial which defines the extension. In the sense of the following theorem, the decomposition of this polynomial into irreducible factors over the residue field $\kappa(\mathfrak{p})$ corresponds to the prime ideal decomposition of $\mathfrak{p}\mathcal{O}_K$.

Theorem 2.1.1.

Let $\theta \in \mathcal{O}_K$ be a primitive element of K with minimal polynomial $h(x) \in \mathcal{O}_k[x]$ and let $f = (\mathcal{O}_K : \mathcal{O}_k[\theta])$. Let \mathfrak{p} be a prime ideal of k prime to $f\mathcal{O}_k$. If the reduction $\overline{h}(x) = h(x) \mod \mathfrak{p}$ has the following decomposition over the residue field $\kappa(\mathfrak{p})$

$$\overline{h}(x) = \overline{h_1}(x)^{e_1} \cdot \ldots \cdot \overline{h_g}(x)^{e_g}$$

into normalized irreducible $\overline{h_i}(x) \in \kappa(\mathfrak{p})[x]$, then the ideal $\mathfrak{p}\mathcal{O}_K$ has the following decomposition over \mathcal{O}_K

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_q^{e_g}$$

into a product of prime ideals \mathfrak{P}_i of \mathcal{O}_K which are given by

$$\mathfrak{P}_i = (\mathfrak{p}, h_i(\theta)) = \mathfrak{p}\mathcal{O}_K + h_i(\theta)\mathcal{O}_K$$

where $h_i(x) \in \mathcal{O}_k[x]$ is a normalized polynomial such that $\overline{h}_i = h_i \mod \mathfrak{p}$. The inertial degrees and ramification indices satisfy

$$f_{K/k}(\mathfrak{P}_i) = \deg \overline{h}_i \quad and \quad e_{K/k}(\mathfrak{P}_i) = e_i.$$

Proof.

See [Neuk92, I. Satz 8.3, I. §8, Aufg. 5] or [Cohe93, Thm. 4.8.13] in the case of $k = \mathbb{Q}$.

When examining the decomposition, we have to disregard finitely many \mathfrak{p} , namely the divisors of the index $f = (\mathcal{O}_K : \mathcal{O}_k[\theta])$. If $d_{K/k}$ denotes the discriminant of the extension K/k, $d_{K/k} = \det((\operatorname{Tr}_{K/k}(\omega_i\omega_j))_{1\leq i,j\leq n})\mathcal{O}_k$ for an integral basis $\{\omega_1, \ldots, \omega_n\}$ of \mathcal{O}_K over \mathcal{O}_k , the discriminant of the minimal polynomial h(x) of θ satisfies (see [Cohe93, Prop. 4.4.4])

$$\operatorname{Dis}(h)\mathcal{O}_k = f^2 d_{K/k}$$

If f = 1, the decomposition behaviour of all prime ideals can be read off from h(x). If f > 1, then we can hope to find another defining polynomial with a more convenient discriminant by choosing another primitive element θ . However, there are extensions for which the index f = 1 cannot be reached (for example [Cohe93, Exer. 6.10]). In this case, any divisor which additionally appears besides $d_{K/k}$ within the discriminants of all possible minimal polynomials is called inessential discriminant divisor. In spite of this problem, using refined methods, it is at least in the case $k = \mathbb{Q}$ possible to algorithmically determine the prime ideal decomposition for all \mathfrak{p} on the basis of the procedure described above (see [Cohe93, Alg. 6.2.9]).

The decomposition of a polynomial into irreducible factors over a finite field can be calculated with a quite modest effort (see [Berl70] and [Cohe93, 3.4]). Thus one gets a simple and effective procedure which provides the decomposition of almost all prime ideals of k. This fact is especially valuable when other results are not yet available.

If K/k is a Galois extension, we can describe the decomposition of a prime ideal \mathfrak{p} of k in terms of the Galois group. For a prime ideal \mathfrak{P} in K lying over \mathfrak{p} we define the *decomposition group* $D_{\mathfrak{P}}$ by

$$D_{\mathfrak{P}} = \{ \sigma \in \operatorname{Gal}(K/k) \mid \sigma(\mathfrak{P}) = \mathfrak{P} \}.$$

 $D_{\mathfrak{P}}$ is the subgroup of those automorphisms of $\operatorname{Gal}(K/k)$ which fix \mathfrak{P} as a set. By passing to the residue field $\kappa(\mathfrak{P})$, any $\sigma \in D_{\mathfrak{P}}$ defines an automorphism $\overline{\sigma}$ of the extension of residue fields $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$. The law $\sigma \mapsto \overline{\sigma}$ provides a surjective group homomorphism $D_{\mathfrak{P}} \to \operatorname{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ whose kernel

 $I_{\mathfrak{P}} = \{ \sigma \in D_{\mathfrak{P}} \mid \sigma(a) \equiv a \mod \mathfrak{P} \text{ for all } a \in \mathcal{O}_K \}$

is called the *inertial group* of \mathfrak{P} . The sizes of these subgroups of $\operatorname{Gal}(K/k)$ satisfy

$$|D_{\mathfrak{P}}| = f_{K/k}(\mathfrak{P}) e_{K/k}(\mathfrak{P})$$
 and $|I_{\mathfrak{P}}| = e_{K/k}(\mathfrak{P})$.

The fixed field $K^{D_{\mathfrak{P}}}$ of $D_{\mathfrak{P}}$ is called the *decomposition field* of \mathfrak{P} . $K^{D_{\mathfrak{P}}}/k$ is the maximal subextension of K/k in which \mathfrak{p} is fully decomposed. Accordingly, the fixed field $K^{I_{\mathfrak{P}}}$ of $I_{\mathfrak{P}}$ is called the *inertial field* of \mathfrak{P} , and $K^{I_{\mathfrak{P}}}/k$ is the maximal subextension of K/k in which \mathfrak{p} is unramified. The factor group $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ is cyclic, since it is isomorphic to the Galois group of the extension $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ of finite fields which is generated by the *Frobenius automorphism* $\pi_{\mathfrak{P}}:\kappa(\mathfrak{P}) \to \kappa(\mathfrak{P}), x \mapsto x^{N(\mathfrak{p})}.$

Proposition 2.1.2.

Let K/k be a Galois extension and \mathfrak{p} a prime ideal of k.

- (a) The Galois group $\operatorname{Gal}(K/k)$ operates transitively on $P_{K/k}(\mathfrak{p})$.
- (b) The decomposition and inertial groups of the prime ideals lying over p are conjugates of each other:

$$D_{\sigma(\mathfrak{P})} = \sigma D_{\mathfrak{P}} \sigma^{-1}$$
 and $I_{\sigma(\mathfrak{P})} = \sigma I_{\mathfrak{P}} \sigma^{-1}$ for all $\sigma \in \operatorname{Gal}(K/k)$.

(c) Inertial degrees and ramification indices of all prime ideals lying over p coincide:

$$e_{K/k}(\sigma(\mathfrak{P})) = e_{K/k}(\mathfrak{P}), f_{K/k}(\sigma(\mathfrak{P})) = f_{K/k}(\mathfrak{P}) \text{ for all } \sigma \in \operatorname{Gal}(K/k).$$

Proof.

(a), (c) see [Neuk92, I. Satz 9.1, I. §9, p. 58], (b) see [Gold71, 5-4-1, 5-4-3]. $\hfill\square$

In the case of Galois extensions K/k we may write $e_{K/k}(\mathfrak{p})$ and $f_{K/k}(\mathfrak{p})$ since these quantities prove to be independent of the prime ideal \mathfrak{P} over \mathfrak{p} by Proposition 2.1.2 (c).

If K/k is a Galois extension with Galois group G then the prime ideal decomposition of \mathfrak{p} is

$$\mathfrak{p}\mathcal{O}_K = \prod_{\sigma \in G/D_\mathfrak{P}} (\sigma(\mathfrak{P}))^e , \qquad e = e_{K/k}(\mathfrak{p}) ,$$

where σ runs through a system of representatives of left cosets of $D_{\mathfrak{P}}$ in G.

If we fix an algebraic closure \overline{k} of k, we will conclude from the Theorem of Bauer (Theorem 2.3.2) that any Galois extension K/k is uniquely determined by its decomposition law. This statement does not hold for general extensions of number fields, as shows the counter-example in [CaFr67, Exercise 6.4, p. 363]. However, from a given decomposition law we are able to read off quantities like the degree of the respective extension and the ramified prime ideals.

In arbitrary extensions of number fields which are not necessarily Galois, the decomposition behaviour of prime ideals can also be described in terms of Galois groups. To do this, we need the following notion.

Let G be a group and U, V subgroups of G. We define an equivalence relation on G by

$$\sigma \sim \tau \iff \tau = u\sigma v \text{ for } u \in U, v \in V.$$

The equivalence classes $U\sigma V$ are called double cosets of G, their totality being denoted by $U \setminus G/V$.

According to [Hupp67, I. 2.19], the size of a double coset satisfies

$$|U\sigma V| = \frac{|U| |V|}{|U \cap \sigma V \sigma^{-1}|}$$

Let L/k be an extension of number fields and N/k a Galois extension satisfying $L \subseteq N$. Let G = Gal(N/k), and let H = Gal(N/L) be the subgroup of G corresponding to the subfield L. If \mathfrak{p} is a prime ideal of k and \mathfrak{P} a prime ideal of N lying over \mathfrak{p} , the following proposition is valid.

Theorem 2.1.2.

Using the notations mentioned above, the following map is a bijection

$$\begin{array}{l} H \backslash G / D_{\mathfrak{P}} \to P_{L/k}(\mathfrak{p}), \\ H \sigma D_{\mathfrak{P}} & \mapsto \sigma \mathfrak{P} \cap L. \end{array}$$

Proof. (cf. [Neuk92, I §9, p. 57f])

(i) Well-definition:

Suppose we have $H\sigma D_{\mathfrak{P}} = H\tau D_{\mathfrak{P}}$, i. e. $\tau = h\sigma d$ with $h \in H$ and $d \in D_{\mathfrak{P}}$. Then we conclude $\tau(\mathfrak{P}) \cap L = h\sigma d(\mathfrak{P}) \cap L = h(\sigma(\mathfrak{P}) \cap L) = \sigma(\mathfrak{P}) \cap L$.

(ii) Injectivity: Suppose we have $\sigma(\mathfrak{P}) \cap L = \tau(\mathfrak{P}) \cap L = \mathfrak{p}_L$. Since $\sigma(\mathfrak{P})$ and $\tau(\mathfrak{P})$ are prime ideals of N lying over \mathfrak{p}_L and H operates transitively on $P_{N/L}(\mathfrak{p}_L)$ (Proposition 2.1.2 (a)), there is a $h \in H$ satisfying $\sigma(\mathfrak{P}) = h\tau(\mathfrak{P})$. We conclude $\tau^{-1}h^{-1}\sigma = d \in D_{\mathfrak{P}}$, that is $\sigma = h\tau d$ and $H\sigma D_{\mathfrak{P}} = H\tau D_{\mathfrak{P}}$.

(iii) Surjectivity:

Let \mathfrak{p}'_L be a prime ideal of L lying over \mathfrak{p} and \mathfrak{P}' a prime ideal of N over \mathfrak{p}'_L . Since G operates transitively on $P_{N/k}(\mathfrak{p})$, there is a $\sigma \in G$ satisfying $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Then we get $\mathfrak{p}'_L = \sigma(\mathfrak{P}) \cap L$. \Box

A system of representatives $\{\sigma_1, \ldots, \sigma_g\}$ of $H \setminus G/D_{\mathfrak{P}}$ corresponds therefore bijectively to the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_g\}$ of prime ideals of L lying over \mathfrak{p} , by means of the map $\sigma_i \mapsto \mathfrak{p}_i = \sigma_i(\mathfrak{P}) \cap L$.

Corollary 2.1.1.

- (a) We have $|H\sigma_i D_{\mathfrak{P}}| = |H| e_{L/k}(\mathfrak{p}_i) f_{L/k}(\mathfrak{p}_i)$.
- (b) \mathfrak{p}_i is unramified in L/k and has inertial degree 1 over \mathfrak{p} if and only if $\sigma_i D_{\mathfrak{P}} \sigma_i^{-1} \subseteq H$.

Proof.

The assertions can be deduced from the formula above for $|U\sigma V|$ using the equality $|H \cap D_{\mathfrak{P}}| = e_{N/L}(\mathfrak{P}) f_{N/L}(\mathfrak{P})$.

2.2 Decomposition in Abelian Extensions

In order to distinguish between finite abelian extensions of a number field k, we use a generalization of the usual notion of congruence from \mathbb{Z} to k^* . We pursue the idea to include the ramification appearing in the extension K/k into the modulus and sift it out before performing further considerations. Standard references for this section are [Hass67] and [Janu73].

Let k be an algebraic number field of absolute degree $[k : \mathbb{Q}] = n < \infty$. A place of k is defined as a class of equivalent valuations of k. Each prime ideal of k determines a class of non-archimedian valuations of k. These classes are called the *finite places* of k, and they are identified with the corresponding prime ideals. \mathfrak{p} is called *infinite place*, written $\mathfrak{p}|\infty$, if \mathfrak{p} forms a class of archimedian valuations. To any infinite place \mathfrak{p} corresponds an embedding $\tau : k \to \mathbb{C}$. $\mathfrak{p}|\infty$ is called *real* if it satisfies $\tau(k) \subset \mathbb{R}$, otherwise \mathfrak{p} is called *complex*. Complex places always appear in pairs which correspond to complex conjugate embeddings. If r_1 denotes the number of real places and r_2 the number of pairs of conjugate complex places, we have

$$r_1 + 2r_2 = n$$

In particular, k possesses only finitely many places $\mathfrak{p}|\infty$.

A modulus \mathfrak{m} is defined to be a formal product of powers of places

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})} , \qquad n(\mathfrak{p}) \in \mathbb{Z}, \ n(\mathfrak{p}) \ge 0, \ n(\mathfrak{p}) \neq 0 \text{ for finitely many } \mathfrak{p}.$$

We additionally require $n(\mathfrak{p}) \leq 1$ for real \mathfrak{p} and $n(\mathfrak{p}) = 0$ for complex \mathfrak{p} .

Any modulus \mathfrak{m} possesses a decomposition $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$ where \mathfrak{m}_0 denotes the finite part of \mathfrak{m} , that is the prime ideal powers appearing in \mathfrak{m} , and \mathfrak{m}_∞ contains the infinite places.

For any place \mathfrak{p} of $k, r \in \mathbb{N}$ and $a, b \in k^*$ we define the *congruence* $a \equiv b \mod \mathfrak{p}^r$ by

$$\frac{a}{b} \equiv 1 \mod \mathfrak{p}^r. \tag{2.2}$$

This notation means the following:

- If \mathfrak{p} is a finite place, we think of k as being embedded in the completion $k_{\mathfrak{p}}$. Then the congruence (2.2) is equivalent to $\frac{a}{b}$ being an element of the valuation ring $R_{\mathfrak{p}}$ of $k_{\mathfrak{p}}$ and we have $\frac{a}{b} - 1 \in M_{\mathfrak{p}}^{r}$ where $M_{\mathfrak{p}}$ denotes the maximal ideal of $k_{\mathfrak{p}}$.
- If \mathfrak{p} is a real place, there is an embedding $\tau : k \to \mathbb{R}$ belonging to \mathfrak{p} . The congruence (2.2) is satisfied if and only if $\tau(\frac{a}{b}) > 0$.
- If \mathfrak{p} is a complex place, the congruence is always satisfied.

For an arbitrary modulus \mathfrak{m} and $a,b\in k^*$ the congruence

$$a \equiv b \mod \mathfrak{m}$$

is satisfied if the congruences $a \equiv b \mod \mathfrak{p}^r$ are satisfied for all powers of places \mathfrak{p}^r appearing in \mathfrak{m} .

Remark 2.2.1.

The validity of the congruence $a \equiv b \mod \mathfrak{m}$ for $a, b \in k^*$ leads to the following consequences:

- 1. If $a\mathcal{O}_k$ and $b\mathcal{O}_k$ are relatively prime to \mathfrak{m} then the congruence is satisfied in the usual sense, i. e. $a - b \in \mathfrak{m}$.
- 2. The prime ideals contained in \mathfrak{m} have to appear in $a\mathcal{O}_k$ and $b\mathcal{O}_k$ to the same power.
- 3. For any real place contained in \mathfrak{m} , a and b have to possess the same sign when embedded into \mathbb{R} via τ .

We use a modulus \mathfrak{m} in order to define the following subgroups of k^* ,

$$k_{\mathfrak{m}} = \{ \frac{a}{b} \in k^* \mid a, b \in \mathcal{O}_k, b \neq 0, \ a\mathcal{O}_k, b\mathcal{O}_k \text{ prime to } \mathfrak{m} \},\$$

$$k_{\mathfrak{m},1} = \{ \frac{a}{b} \in k_{\mathfrak{m}} \mid \frac{a}{b} \equiv 1 \mod \mathfrak{m} \}.$$

We notice that $k_{\mathfrak{m}}$ only depends on the finite places of k but not on their exponents. The elements of $k_{\mathfrak{m}}$ are the numbers of k which have a representation as a fraction whose numerator and denominator generate principal ideals prime to \mathfrak{m} . $k_{\mathfrak{m},1}$ is called the *ray modulo* \mathfrak{m} . The proposition below says that to any given modulus \mathfrak{m} in k^* there are only finitely many congruence classes, i. e. cosets of the ray modulo \mathfrak{m} .

Proposition 2.2.1.

If r denotes the number of real places in \mathfrak{m} and $N = N_{k/\mathbb{Q}} : k \to \mathbb{Q}$ the norm map then the index $\varphi(\mathfrak{m})$ of $k_{\mathfrak{m},1}$ in $k_{\mathfrak{m}}$ satisfies

$$\varphi(\mathfrak{m}) \ = \ \left(\ k_{\mathfrak{m}} \ : \ k_{\mathfrak{m},1} \ \right) \ = \ 2^r N(\mathfrak{m}_0) \prod_{\mathfrak{p} \mid \mathfrak{m}_0} \left(1 - \frac{1}{N(\mathfrak{p})} \right).$$

Proof.

See [Hass67, Satz (48)].

The absolute ideal group I_k of k is the free abelian group generated by the prime ideals of k,

$$I_k = \{ \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})} \mid \mathfrak{p} \text{ prime ideal of } k, a(\mathfrak{p}) \in \mathbb{Z}, a(\mathfrak{p}) \neq 0 \text{ for finitely many } \mathfrak{p} \}.$$

Using the map $i: k^* \to I_k$, $a \mapsto a\mathcal{O}_k$ which assigns to any field element different from zero the principal ideal generated by it, we get the exact sequence

$$1 \to \mathcal{O}_k^* \to k^* \to I_k \to \operatorname{Cl}(k) \to 1,$$

where $\operatorname{Cl}(k) = I_k/i(k^*)$ denotes the *class group* of k. It is a fundamental result of algebraic number theory that $\operatorname{Cl}(k)$ is always a finite abelian group. Its size h_k is called the *class number* of the number field k.

If S is a finite set of prime ideals of k, I_k^S is the subgroup of I_k generated by all prime ideals not lying in S. Specifically, given any modulus \mathfrak{m} of k, the group $I_k^{\mathfrak{m}}$ is generated by all prime ideals of \mathcal{O}_k which do not appear in \mathfrak{m} . In this case S is the set of all prime ideals which divide \mathfrak{m}_0 .

From the next proposition we may conclude that using such a set S we can exclude finitely many prime ideals from I_k without any ideal class getting empty; in other words, each ideal class contains ideals which are not divided by any prime ideal contained in S.

Proposition 2.2.2.

Let S be a finite set of prime ideals. Then it holds $\operatorname{Cl}(k) \cong I_k^S/(I_k^S \cap i(k^*))$.

Proof.

See [Janu73, IV 1.5].

The factor group $\operatorname{Cl}_{\mathfrak{m}}(k) = I_k^{\mathfrak{m}}/i(k_{\mathfrak{m},1})$ is called *ray class group modulo* \mathfrak{m} .

Proposition 2.2.3.

The ray class group modulo \mathfrak{m} is finite for any modulus \mathfrak{m} over k. Its size is given by

$$h_{k,\mathfrak{m}} = (I_k^{\mathfrak{m}} : i(k_{\mathfrak{m},1})) = h_k \frac{\varphi(\mathfrak{m})}{w_{\mathfrak{m}}}$$

where $w_{\mathfrak{m}}$ denotes the number of classes modulo \mathfrak{m} which contain units of the ring of integers \mathcal{O}_k .

Proof. See [Hass67, Satz (52)].

A subgroup H of I_k is defined modulo \mathfrak{m} if we have $i(k_{\mathfrak{m},1}) \leq H \leq I_k^{\mathfrak{m}}$. \mathfrak{m} is called a modulus of definition for H. The factor group $I_k^{\mathfrak{m}}/H$ is called generalized ideal class group for the modulus \mathfrak{m} . It is finite since it is a factor group of $\operatorname{Cl}_{\mathfrak{m}}(k)$.

Proposition 2.2.4.

- (a) Let m, n be moduli of k such that n|m, and let H^m, Hⁿ be subgroups of I_k defined modulo m and modulo n, respectively, satisfying H^m = I_k^m ∩ Hⁿ. Then we have I_k^m/H^m ≅ I_kⁿ/Hⁿ and Hⁿ = H^m i(k_{n,1}).
- (b) Let H₁, H₂ be defined modulo m₁ and modulo m₂, respectively, and assume we have some modulus n with H₁ ∩ Iⁿ_k = H₂ ∩ Iⁿ_k. Then for the modulus m = gcd(m₁, m₂) there exists a subgroup H of I_k defined modulo m satisfying H ∩ I^{m_i}_k = H_i, i = 1, 2.

Proof.

See [Janu73, V 6.1, V 6.2].

We define an equivalence relation on the subgroups of I_k by the rule:

 $H_1 \sim H_2$ holds if and only if there is a modulus \mathfrak{m} such that H_1 and H_2 are defined modulo \mathfrak{m} and satisfy $H_1 \cap I_k^{\mathfrak{m}} = H_2 \cap I_k^{\mathfrak{m}}$.

Any class of this equivalence relation is called an *ideal group*. Proposition 2.2.4 states that in each ideal group H we find a unique representative $H^{\mathfrak{f}}$ having the modulus of definition \mathfrak{f} such that any further element $H^{\mathfrak{m}} \in H$ with modulus of definition \mathfrak{m} satisfies the relation $\mathfrak{f}|\mathfrak{m}$. The modulus $\mathfrak{f} = \mathfrak{f}(H)$ is called the *conductor* of the ideal group H.

The ideal group H_1 is called *subgroup* of the ideal group H_2 (written as $H_1 \leq H_2$) if there exist some modulus \mathfrak{m} and some representatives $H_1^{\mathfrak{m}} \in H_1$ and $H_2^{\mathfrak{m}} \in H_2$ which are defined modulo \mathfrak{m} and satisfy $H_1^{\mathfrak{m}} \leq H_2^{\mathfrak{m}}$. Similarly, we introduce intersections and spans of ideal groups. The ideal \mathfrak{a} of I_k is an element of the ideal group H if and only if we have $\mathfrak{a} \in H^{\mathfrak{f}(H)}$. By Proposition 2.2.4 (a) we may define for any ideal group H its factor group I_k/H by choosing any representative $H^{\mathfrak{m}}$ of H with modulus of definition \mathfrak{m} and setting I_k/H equal to $I_k^{\mathfrak{m}}/H^{\mathfrak{m}}$.

Proposition 2.2.5.

Let H_1, H_2 be ideal groups of k with $H_1 \leq H_2$. Then their conductors satisfy $\mathfrak{f}(H_2) | \mathfrak{f}(H_1)$.

Proof.

See [Hass67, p. 80, following Def. (62)].

Let L/k be a finite Galois extension, \mathfrak{p} an unramified prime ideal of k, and \mathfrak{P} a prime ideal of L over \mathfrak{p} . Then the decomposition group $D_{\mathfrak{P}}$ of \mathfrak{P} is a cyclic subgroup of $\operatorname{Gal}(L/k)$ isomorphic to the Galois group $\operatorname{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ which is generated by the Frobenius automorphism $\pi_{\mathfrak{P}}$. The preimage of $\pi_{\mathfrak{P}}$ under the isomorphism of the Galois groups just mentioned is the automorphism of L which is uniquely determined by the condition $\alpha \mapsto \alpha^{N(\mathfrak{p})} \mod \mathfrak{P}$. This automorphism is denoted by the Artin symbol $\left(\frac{L/k}{\mathfrak{P}}\right)$. We have $\left(\frac{L/k}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/k}{\mathfrak{P}}\right)\sigma^{-1}$ for any $\sigma \in \operatorname{Gal}(L/k)$, i. e. the Artin symbols corresponding to the prime ideals of L lying over \mathfrak{p} are conjugate under $\operatorname{Gal}(L/k)$. They even form a whole conjugacy class in $\operatorname{Gal}(L/k)$,

$$C(\mathfrak{p}) = \left\{ \left(\frac{L/k}{\mathfrak{P}} \right) \mid \mathfrak{P} \in P_{L/k}(\mathfrak{p}) \right\}.$$

If $\operatorname{Gal}(L/k)$ is abelian then the Artin symbols of all prime ideals lying over \mathfrak{p} are mapped to the same automorphism which is then denoted by $\left(\frac{L/k}{\mathfrak{p}}\right)$. $\left(\frac{L/k}{\mathfrak{p}}\right)$ is uniquely determined by the rule $\alpha \mapsto \alpha^{N(\mathfrak{p})} \mod \mathfrak{p}\mathcal{O}_L$. Let K/k be a finite abelian extension and \mathfrak{m} a modulus of k which is divisible by all places ramified in K/k. We define the Artin map

$$\varphi_{K/k}^{\mathfrak{m}}: I_k^{\mathfrak{m}} \to \operatorname{Gal}(K/k)$$

by assigning to each prime ideal \mathfrak{p} of $I_k^{\mathfrak{m}}$ its Artin symbol $\left(\frac{K/k}{\mathfrak{p}}\right)$ and by extending the map multiplicatively to all of $I_k^{\mathfrak{m}}$.

Hence the Artin map assigns to any product of unramified prime ideals the composition of the respective Frobenius automorphisms, and this rule gives a well-defined group homomorphism because $\operatorname{Gal}(K/k)$ is abelian.

If \mathfrak{p} is an unramified prime ideal of k with relative inertial degree f, \mathfrak{p}^f lies in the kernel of the Artin map, and \mathfrak{p}^f is the norm of each prime ideal of K lying over \mathfrak{p} . Thus we have

$$N_{K/k}(I_K^{\mathfrak{m}}) \subseteq \ker \varphi_{K/k}^{\mathfrak{m}},$$

where \mathfrak{m} is viewed as a modulus over K in the obvious way.

It is a main result of class field theory that the kernel of the Artin map contains all principal ideals $\alpha \mathcal{O}_k$ satisfying $\alpha \equiv 1 \mod \mathfrak{m}$ for a suitably chosen modulus \mathfrak{m} . More precisely, we have the following theorem (which can be viewed as a generalization of the Quadratic Reciprocity Law).

Theorem 2.2.1. (Artin Reciprocity Law)

Let K/k be a finite abelian extension. Let the modulus \mathfrak{m} of k be divisible by all places of k ramified in K/k, and assume the exponents appearing in \mathfrak{m} are sufficiently large. Then we have

$$\ker \varphi_{K/k}^{\mathfrak{m}} = N_{K/k}(I_{K}^{\mathfrak{m}}) \ i(k_{\mathfrak{m},1}) \quad and \quad I_{k}^{\mathfrak{m}}/\ker \varphi_{K/k}^{\mathfrak{m}} \cong \operatorname{Gal}(K/k).$$

Proof.

See [Janu73, V 5.7]. The surjectivity of the isomorphism induced by the Artin map is concluded by a density argument, similar to the Theorem of Chebotarev (Theorem 2.3.1). $\hfill \Box$

The next proposition states that there is a unique smallest modulus \mathfrak{m} of k satisfying the conditions of Theorem 2.2.1.

Theorem 2.2.2. (Conductor-Ramification-Theorem)

Let K/k be a finite abelian extension. Then there is a modulus $\mathfrak{f} = \mathfrak{f}(K/k)$ of k, called the conductor of the extension K/k, with the following properties.

- (a) A place \mathfrak{p} of k is ramified in K if and only if we have $\mathfrak{p} \mid \mathfrak{f}$.
- (b) Let m be a modulus of k which is divisible by all places p of k ramified in K. ker φ^m_{K/k} is defined modulo m if and only if we have f | m.

Proof.

```
See [Hass67, II, §10, II., p. 136], [Janu73, V §6].
```

16 2 Decomposition Laws

To any finite abelian extension K/k we assign an ideal group H(K/k) by the rule

$$H(K/k) = [N_{K/k}(I_K^{f(K/k)}) i(k_{f(K/k),1})]_{\sim} , \qquad (2.3)$$

where $[]_{\sim}$ denotes a class of the equivalence relation described directly after Proposition 2.2.4. By Theorem 2.2.2 we have f(H(K/k)) = f(K/k).

By definition of the Artin map and by Theorem 2.2.1, the set of prime ideals contained in H(K/k) is equal to the set S(K/k) of fully decomposed prime ideals of k,

$$H(K/k) \cap \{ \mathfrak{p} \mid \mathfrak{p} \text{ prime ideal in } k \} = S(K/k).$$

The Galois group of K/k is rediscovered as a quotient of the absolute ideal group I_k . We have

$$\operatorname{Gal}(K/k) \cong I_k/H(K/k)$$

where the isomorphism is given by the Artin map as in Theorem 2.2.1.

Proposition 2.2.6. (Classification of Abelian Extensions)

Let k be an algebraic number field. Then there is a bijective, inclusion reversing correspondence between finite abelian extensions of k and ideal groups of k, given by the rule $K \mapsto H(K/k)$.

Proof.

See [Janu73, V 9.16].

As a consequence of Proposition 2.2.6 and Theorem 2.2.1, the Galois group of every abelian extension of k appears as a factor group of some ray class group $\operatorname{Cl}_{\mathfrak{m}}(k)$, i. e. every abelian extension K/k is contained in some ray class extension $K_{\mathfrak{m}}/k$ corresponding to $H(K_{\mathfrak{m}}/k) = i(k_{\mathfrak{m},1})$. Appropriate moduli \mathfrak{m} of k are all multiples of the conductor $\mathfrak{f}(K/k)$. This statement generalizes the Theorem of Kronecker-Weber asserting that every abelian extension of \mathbb{Q} is contained in some cyclotomic extension $\mathbb{Q}(\mu_m)/\mathbb{Q}$.

In order to determine the conductor of the extension K/k having the ideal group H = H(K/k), we may use the characters χ of I_k/H . We identify χ with its canonical lifting to $I_k^{\mathfrak{m}}$ for some modulus of definition \mathfrak{m} of H. χ is assigned to the ideal group

$$H_{\chi} = \left[\left\{ \mathfrak{a} \in I_k^{\mathfrak{m}} \mid \chi(\mathfrak{a}) = 1 \right\} \right]_{\sim}$$

with conductor $\mathfrak{f}_{\chi} = \mathfrak{f}(H_{\chi})$. By definition of the character we have $H \leq H_{\chi}$. Furthermore, I_k/H_{χ} is cyclic, thus the abelian extension K_{χ}/k , which is uniquely determined by H_{χ} by Proposition 2.2.6, is a cyclic subextension of K/k. The following theorem provides a classical result which reduces the problem of calculating the conductor and the discriminant of an abelian extension to cyclic extensions.

Theorem 2.2.3. (Conductor-Discriminant-Formulas)

Let $d_{K/k}$ denote the discriminant of the extension K/k. Then we have

$$d_{K/k} = \prod_{\chi \in \widehat{I_k/H}} (\mathfrak{f}_{\chi})_0 \quad , \qquad \mathfrak{f}(K/k) = \underset{\chi \in \widehat{I_k/H}}{\operatorname{kgV}} \mathfrak{f}_{\chi} \quad .$$

Proof.

See [Hass67, II, §10, III., p. 136].

Our next aim is to state the decomposition law of finite abelian extensions of a number field. We will recognize that in the extension K/k the decomposition behaviour of a prime ideal \mathfrak{p} of k depends only on its ideal class, i. e. on the coset of H(K/k) belonging to \mathfrak{p} .

Let $\mathfrak{f} = \mathfrak{f}(K/k)$ be the conductor of the extension K/k, and let $H^{\mathfrak{f}}$ be the representative of the ideal group H = H(K/k) defined modulo \mathfrak{f} . Let \mathfrak{p} be a prime ideal of k. Then let $H_{\mathfrak{p}}$ denote the smallest ideal group containing $H^{\mathfrak{f}}$ having a conductor coprime to \mathfrak{p} . $H_{\mathfrak{p}}$ is the intersection of all ideal groups which contain $H^{\mathfrak{f}}$ and which have a conductor coprime to \mathfrak{p} . This description makes sense by Proposition 2.2.5 because I_k appears as one of the sets to be intersected.

Using the correspondence of Proposition 2.2.6, $H_{\mathfrak{p}}$ belongs to the inertial field of \mathfrak{p} , i. e. to the maximal subextension of K/k in which \mathfrak{p} remains unramified. In particular, we have $H_{\mathfrak{p}} = H$, if \mathfrak{p} is unramified in K/k.

Theorem 2.2.4. (Decomposition Law in Abelian Extensions)

Let K/k be a finite abelian extension of number fields, and let \mathfrak{p} be a prime ideal of k. Let $e = (H_{\mathfrak{p}} : H)$, and let f denote the order of $\mathfrak{p}H_{\mathfrak{p}}$ in $I_k/H_{\mathfrak{p}}$, i. e. the smallest natural number f with $\mathfrak{p}^f \in H_{\mathfrak{p}}$. Then we have

$$\mathfrak{p}\mathcal{O}_K = (\mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_g)^e$$
 with $f_{K/k}(\mathfrak{p}) = f$ and $g = \frac{[K:k]}{ef}$.

Proof.

See [Hass67, II, §10, IVa., p. 137].

Kummer extensions are a special case of abelian extensions. Their shape enables a simpler classification, and the statements on general abelian extensions can be reduced to this particular type of extensions.

Let $n \in \mathbb{N}$. A finite Galois extension K/k of algebraic number fields is called *n*-th *Kummer extension* if *k* contains the group μ_n of *n*-th roots of unity and the Galois group of K/k has the exponent *n*, i. e. $\sigma^n = id$ holds for all $\sigma \in \text{Gal}(K/k)$.

The proposition below asserts that *n*-th Kummer extensions correspond bijectively to finite subgroups of k^*/k^{*n} .

17

Proposition 2.2.7. (Classification of Kummer Extensions)

Let $n \in \mathbb{N}$, let k contain the n-th roots of unity. Then there is a bijective, inclusion preserving correspondence between n-th Kummer extensions K/kand groups W with $k^{*n} \leq W < k^*$ whose factor group W/k^{*n} is finite, given by

$$K \mapsto W(K/k) = K^{*n} \cap k,$$

$$W \mapsto K(W) = k \left(\sqrt[n]{W}\right).$$

The Galois group of the n-th Kummer extension K/k satisfies

$$\operatorname{Gal}(K/k) \cong W(K/k)/k^{*n}.$$

Proof.

See [Janu73, V 8.1] or [Neuk92, IV. Theorem 3.3].

Cyclic Kummer extensions K/k have the form $K = k(\sqrt[n]{a})$ for an element $a \in k^*$. Their Galois groups are cyclic, and we get a monomorphism $\operatorname{Gal}(k(\sqrt[n]{a})/k) \to \mu_n$ by $\sigma \mapsto \sigma(\sqrt[n]{a})/\sqrt[n]{a}$, i. e. we may interpret the operation of the Galois group as multiplication by roots of unity. Any general Kummer extension can be expressed as a composite of linear disjoint cyclic Kummer extensions.

We obtain the same extension $k(\sqrt[n]{a})/k$, if we replace the element $a \in k^*$ by certain other elements of the multiplicative subgroup of k^* generated by aand k^{*n} . More precisely, we have $k(\sqrt[n]{a}) = k(\sqrt[n]{b})$ if and only if b has the form $b = a^r c^n$ with $c \in k^*$ and $r \in \mathbb{Z}$ satisfying gcd(r, n) = 1. We may therefore assume without loss of generality that we have $a \in \mathcal{O}_k$ and that every prime factor of $a\mathcal{O}_k$ appears at most to the (n-1)-st power. Since the discriminant of $k(\sqrt[n]{a})/k$ is a divisor of $n^n a^{n-1}$ (see [Bir67, 2., Lemma 5]), each prime ideal \mathfrak{p}/n of k is at most tamely ramified. In the following proposition we state the decomposition law in cyclic Kummer extensions for unramified prime ideals.

Theorem 2.2.5.

(Decomposition Law in Cyclic Kummer Extensions)

Let k be an algebraic number field containing the n-th roots of unity μ_n , let $N = N_{k/\mathbb{Q}} : k \to \mathbb{Q}$ be the absolute norm map and $K = k(\sqrt[n]{a})$. Let $\mathfrak{p} \not\mid na$ be a prime ideal of k. Let

f denote the order of
$$a \frac{N(\mathfrak{p}) - 1}{n}$$
 in $(\mathcal{O}_k/\mathfrak{p})^*$.

Then we have $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_g$ with $f_{K/k}(\mathfrak{p}) = f$ and $g = \frac{[K:k]}{f}$.

Proof. (inspired by [Cox89, Ex. 5.13, Thm. 8.11])

Suppose \mathfrak{p}/n . Then μ_n is a subgroup of $(\mathcal{O}_k/\mathfrak{p})^*$, since μ_n is contained in \mathcal{O}_k by assumption, and the polynomial $X^n - 1$ in $\mathcal{O}_k/\mathfrak{p}$ has no roots in common with its derivative nX^{n-1} . Thus the *n*-th roots of unity are mapped into distinct residue classes by the canonical projection $\mathcal{O}_k \to \mathcal{O}_k/\mathfrak{p}$. $n = |\mu_n|$ is therefore a divisor of $N(\mathfrak{p}) - 1 = |(\mathcal{O}_k/\mathfrak{p})^*|$.

If \mathfrak{p} is ramified in K/k then the polynomial $X^n - a$ has a common factor of degree ≥ 1 with its derivative nX^{n-1} in $\mathcal{O}_k/\mathfrak{p}$ (see Theorem 2.1.1). This can only happen if \mathfrak{p} appears within the prime decomposition of $n\mathcal{O}_k$ or $a\mathcal{O}_k$. Thus \mathfrak{p} is unramified by assumption.

Choose any $\alpha \in K$ with $\alpha^n = a$. Then we have $\left(\frac{K/k}{\mathfrak{p}}\right)(\alpha) = \zeta_{\mathfrak{p}} \cdot \alpha$ for some *n*-th root of unity $\zeta_{\mathfrak{p}}$. The order of $\zeta_{\mathfrak{p}}$ is equal to the order of $\left(\frac{K/k}{\mathfrak{p}}\right)$ in Gal(K/k) which is equal to $f_{K/k}(\mathfrak{P})$ for each prime ideal \mathfrak{P} of K lying over \mathfrak{p} . By the above arguments, the order of $\zeta_{\mathfrak{p}}$ remains unchanged under the projection $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ since \mathfrak{p} is no divisor of n. The properties of the Frobenius automorphism give $\zeta_{\mathfrak{p}} \cdot \alpha \equiv \alpha^{N(\mathfrak{p})} \mod \mathfrak{p}$, hence

$$\zeta_{\mathfrak{p}} \equiv a \frac{N(\mathfrak{p}) - 1}{n} \mod \mathfrak{p}.$$

Therefore, $f_{K/k}(\mathfrak{p})$ is equal to the order of $a^{\frac{N(\mathfrak{p})-1}{n}}$ in $(\mathcal{O}_k/\mathfrak{p})^*$.

Remark 2.2.2. (vgl. [Bir67, 2., Lemma 6]) More generally, let \mathfrak{p} be a prime ideal of k with \mathfrak{p}/n . Let $r \in \mathbb{Z}, 0 \leq r \leq n-1$, be the unique power satisfying $\mathfrak{p}^r|a$ and \mathfrak{p}^{r+1}/a . Then for $s = \gcd(r, n)$ the subfield $L = k(\sqrt[s]{a})$ of $K = k(\sqrt[s]{a})$ is the inertial field of \mathfrak{p} , i. e. \mathfrak{p} is unramified in L/k, and the prime ideals \mathfrak{p}_i of L lying over \mathfrak{p} are totally ramified in K/L. If we denote by

e the order of
$$a^s$$
 in k^*/k^{*n} ,
f the inertial degree of $\mathfrak{p}_i/\mathfrak{p}$ in $k(\sqrt[s]{a})/k_i$

then we have
$$\mathfrak{p}\mathcal{O}_K = (\mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_g)^e$$
 with $f_{K/k}(\mathfrak{p}) = f$ and $g = \frac{[K:k]}{ef}$.

Let k be an algebraic number field containing μ_n , let \mathfrak{p} be a prime ideal of k not dividing n, and let $a \in k^*$ be chosen such that \mathfrak{p} does not appear in the prime ideal decomposition of $a\mathcal{O}_k$. Then we may define the *n*-th power residue symbol $\left(\frac{a}{\mathfrak{p}}\right)_{n,k}$ by

$$\left(\frac{a}{\mathfrak{p}}\right)_{n,k} = \zeta \in \mu_n \subseteq k \text{, where } \zeta \equiv a^{\frac{N(\mathfrak{p})-1}{n}} \mod \mathfrak{p} \text{ in } (\mathcal{O}_k/\mathfrak{p})^*.$$
(2.4)

This notion is linearly extended to ideals \mathfrak{b} of k which are relatively prime to $a\mathcal{O}_k$ and $n\mathcal{O}_k$ by setting

$$\left(\frac{a}{\mathfrak{b}}\right)_{n,k} = \prod_{\mathfrak{p}} \left(\frac{a}{\mathfrak{p}}\right)_{n,k}^{m_{\mathfrak{p}}} \quad \text{if} \quad \mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}} .$$
(2.5)

If there is no risk of confusion, we will drop the index k.

We notice that the order of $\left(\frac{a}{p}\right)_{n,k}$ in μ_n is equal to the inertial degree of \mathfrak{p} in the extension $k(\sqrt[n]{a})/k$.

Some of the most important properties of the n-th power residue symbol are summarized in the following proposition.

Proposition 2.2.8.

Let k be an algebraic number field with $\mu_n \subset k$. Let \mathfrak{a} and \mathfrak{b} be ideals of k which are relatively prime to $n\mathcal{O}_k$.

(a) The n-th power residue symbol is multiplicative in both arguments,

$$\left(\frac{ac}{\mathfrak{a}}\right)_n = \left(\frac{a}{\mathfrak{a}}\right)_n \left(\frac{c}{\mathfrak{a}}\right)_n \quad and \quad \left(\frac{a}{\mathfrak{a}\mathfrak{b}}\right)_n = \left(\frac{a}{\mathfrak{a}}\right)_n \left(\frac{a}{\mathfrak{b}}\right)_n,$$

if $a, c \in k^*$ are relatively prime to \mathfrak{a} or \mathfrak{ab} , respectively.

(b) If $\mu_{nm} \subset k$ then for $a \in k^*$ relatively prime to \mathfrak{b} we have

$$\left(\frac{a}{\mathfrak{b}}\right)_{nm}^m = \left(\frac{a}{\mathfrak{b}}\right)_n.$$

(c) If K is a finite extension of k and $a \in K^*$ is relatively prime to \mathfrak{bO}_K then

$$\left(\frac{a}{\mathfrak{b}\mathcal{O}_K}\right)_{n,K} = \left(\frac{N_{K/k}(a)}{\mathfrak{b}}\right)_{n,K}.$$

(d) If K is a finite extension of k and \mathfrak{B} is an ideal of K relatively prime to $n\mathcal{O}_K$ and $a \in k^*$ is chosen such that $a\mathcal{O}_K$ is relatively prime to \mathfrak{B} then

$$\left(\frac{a}{\mathfrak{B}}\right)_{n,K} = \left(\frac{a}{N_{K/k}(\mathfrak{B})}\right)_{n,k}.$$

Proof.

(a) and (b) are obvious from (2.4) and (2.5). (c) see [Hass65, $\S14$, 2.], (d) see [Hass65, $\S10$, (8.)].

By (c) and (d) of Proposition 2.2.8, the *n*-th power residue symbol can also be given a meaning for number fields k which do not contain μ_n if one of the arguments is the norm of some element or ideal in $k(\mu_n)$. We can no longer identify the value of such a symbol with an element of k, but the order of this symbol in μ_n is well-defined. More specifically, if p is a prime number with $p \equiv 1 \mod n$ and $a \in \mathbb{Z}$ satisfies (a, pn) = 1, we have

$$\left(\frac{a}{p}\right)_n = 1 \iff a \equiv x^n \mod p \text{ has a solution } x \in \mathbb{Z},$$

because there is a prime ideal \mathfrak{p} in $\mathbb{Q}(\mu_n)$ with $N(\mathfrak{p}) = p$.

In the case of a *cyclotomic extension*, which is formed by adjoining some roots of unity, we are able to describe its decomposition law more explicitly than in Theorem 2.2.4. We initially restrict ourselves to the field $k = \mathbb{Q}$. The extension $\mathbb{Q}(\mu_n)/\mathbb{Q}$, which is formed by adjoining μ_n , is a Galois extension of degree $\varphi(n)$ (where φ denotes Euler's totient function), its Galois group being isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$.

Theorem 2.2.6. (Decomposition Law in Cyclotomic Extensions) Let $n = \prod_{p} p^{\nu_{p}}$ be the prime factor decomposition of n. Let $\mathcal{O}_{n} = \mathcal{O}_{\mathbb{Q}(\mu_{n})}$ denote the ring of integers of $\mathbb{Q}(\mu_{n})$. Given a prime number p, we set $e = \varphi(p^{\nu_{p}})$ and define f to be the order of p in $(\mathbb{Z}/\frac{n}{p^{\nu_{p}}}\mathbb{Z})^{*}$, that is the smallest natural number f with $p^{f} \equiv 1 \mod \frac{n}{p^{\nu_{p}}}$. In $\mathbb{Q}(\mu_{n})$ we then have the decomposition

$$p\mathcal{O}_n = (\mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_g)^e$$

into different prime ideals \mathfrak{P}_i with inertial degree $f_{\mathbb{Q}(\mu_n)/\mathbb{Q}}(p) = f$.

Proof.

See [Neuk92, I. Satz 10.3].

We finish this section by stating an important corollary which extends this result to number fields k satisfying $k \cap \mathbb{Q}(\mu_n) = \mathbb{Q}$.

Corollary 2.2.1.

Let k be an algebraic number field satisfying $k \cap \mathbb{Q}(\mu_n) = \mathbb{Q}$. Let \mathfrak{p} be a prime ideal of k with $N(\mathfrak{p}) = q$ and (q, n) = 1. We let f be the order of q in $(\mathbb{Z}/n\mathbb{Z})^*$, that is the smallest natural number f with $q^f \equiv 1 \mod n$. Then we have the decomposition

$$\mathfrak{p}\mathcal{O}_{k(\mu_n)} = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_g$$

into different prime ideals \mathfrak{P}_i of $k(\mu_n)$ with inertial degree $f_{k(\mu_n)/k}(\mathfrak{p}) = f$.

Proof.

By assumption we have $\operatorname{Gal}(k(\mu_n)/k) \cong \operatorname{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$, the automorphism σ_a , which corresponds to $a \in (\mathbb{Z}/n\mathbb{Z})^*$, being determined by $\zeta \mapsto \zeta^a$ for some primitive *n*-th root of unity ζ . $f_{k(\mu_n)/k}(\mathfrak{p})$ is equal to the order of the Frobenius element $\sigma_{\mathfrak{p}}$ corresponding to \mathfrak{p} which is determined by $\zeta \mapsto \zeta^q$. Hence we get our assertion. \Box

21

2.3 Density Statements

The methods of class field theory described in the preceding section which lead to a satisfactory statement of the decomposition law in abelian extensions cannot be generalized to arbitrary extensions of number fields. For example, if we are given an arbitrary Galois extension L/k and assign to it its ideal group H(L/k) by (2.3), H(L/k) is equal to the ideal group of the maximal abelian subextension K/k of L/k. Thus, for the Galois group G = Gal(L/k), we get the relation $H(L/k) = H(K/k) \cong G/G'$ with the commutator subgroup G' of G. Theorem 2.2.4 provides therefore only the decomposition law of the abelian subextension K/k of L/k.

If we try to extend the investigation to general Galois extensions, we encounter the basic problem that ideal groups are always abelian groups. In order to map an arbitrary Galois group isomorphically to suitable internal structures of the base field, we have to look for non-abelian groups, for example matrix groups, or we have to consider results of representation theory to find appropriate structures and invariants.

Another possibility is to neglect the abelian structure of the ideal groups and to characterize the extension fields simply by subsets of prime ideals of the base field. This approach leads indeed to more general statements, if we introduce a notion of density to sets of prime ideals which essentially measures the portion of a given set of prime ideals with respect to the set of all prime ideals.

Let \mathfrak{M} be a set of prime ideals of k. We say, \mathfrak{M} has Dirichlet density $\delta_D(\mathfrak{M})$, if the limit

$$\delta_D(\mathfrak{M}) = \lim_{s \to 1^+} \frac{\log \prod_{\mathfrak{p} \in \mathfrak{M}} (1 - N(\mathfrak{p})^{-s})^{-1}}{\log \prod_{\text{all } \mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}} = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathfrak{M}} N(\mathfrak{p})^{-s}}{\sum_{\text{all } \mathfrak{p}} N(\mathfrak{p})^{-s}}$$

(formed for real s > 1) exists. In this case, we have $0 \le \delta_D(\mathfrak{M}) \le 1$.

Similarly, \mathfrak{M} has natural density $\delta_n(\mathfrak{M})$, if the following limit exists

$$\delta_n(\mathfrak{M}) = \lim_{x \to \infty} \frac{|\{ \mathfrak{p} \in \mathfrak{M} \mid N(\mathfrak{p}) \le x \}|}{|\{ \text{ all } \mathfrak{p} \mid N(\mathfrak{p}) \le x \}|}.$$

The connection between these two notions of density is given by the next proposition.

Proposition 2.3.1.

Let \mathfrak{M} be a set of prime ideals of the number field k. If the natural density $\delta_n(\mathfrak{M})$ exists then the Dirichlet density $\delta_D(\mathfrak{M})$ also exists, and they satisfy $\delta_D(\mathfrak{M}) = \delta_n(\mathfrak{M})$.

Proof. See [Hass67, Def. (84), II §8, p. 120f].

Thus, the two notions of density coincide whenever they are both defined. Dirichlet density, however, is the more comprehensive notion (Example: The set of prime numbers having leading digit 1, see [Serr73, VI 4.5, p. 76]).

By means of analytical methods we try to ensure the existence and to calculate the value of the Dirichlet density of a certain given set of prime ideals \mathfrak{M} . We are always permitted to neglect any subset of Dirichlet density 0 (especially any finite subset).

If L/k is a Galois extension and \mathfrak{p} is an unramified prime ideal of k, the Frobenius elements $\left(\frac{L/k}{\mathfrak{P}}\right)$ of all prime ideals \mathfrak{P} of L lying over \mathfrak{p} form a conjugacy class $C(\mathfrak{p})$ of $\operatorname{Gal}(L/k)$. The following Density Theorem of Chebotarev asserts that the set of prime ideals of k, whose Frobenius elements lie in a given conjugacy class C, has strictly positive Dirichlet density, and that the distribution of Frobenius elements corresponding to the prime ideals of k over the conjugacy classes of $\operatorname{Gal}(L/k)$ asymptotically coincides with an equidistribution.

Theorem 2.3.1. (Chebotarev Density Theorem)

Let L/k be a Galois extension of degree n and C a conjugacy class of $\operatorname{Gal}(L/k)$. Let

$$\mathfrak{M}(C) = \{ \mathfrak{p} \mid \mathfrak{p} \text{ unramified in } L/k, \left(\frac{L/k}{\mathfrak{P}}\right) \in C \text{ for all } \mathfrak{P} \text{ over } \mathfrak{p} \}.$$

Then we have $\delta_D(\mathfrak{M}(C)) = \frac{|C|}{n}$.

Proof.

See [Gold71, 9-3] or [Neuk92, VII. Theorem 13.4].

One important consequence of Theorem 2.3.1 is the fact that for any given Galois extension L/k, the set

 $S(L/k) = \{ \mathfrak{p} \text{ prime ideal of } k \mid \mathfrak{p} \text{ fully decomposed in } L/k \}.$

of fully decomposed prime ideals of k has strictly positive Dirichlet density, so that it contains in particular infinitely many elements.

Proposition 2.3.2.

Let L/k be a Galois extension of algebraic number fields. Then the set of fully decomposed prime ideals with respect to L/k satisfies $\delta_D(S(L/k)) = \frac{1}{[L:k]}$.

Proof.

If the prime ideal \mathfrak{p} of k is fully decomposed, it holds $\left(\frac{L/k}{\mathfrak{P}}\right) = \mathrm{id}_L$ for all prime ideals \mathfrak{P} of L over \mathfrak{p} . The result then follows from Theorem 2.3.1 with $C = \{\mathrm{id}_L\}$. See also [Gold71, Thm. 9-1-2].

An immediate consequence of the last two results is the Theorem of Bauer.

Theorem 2.3.2. (Bauer)

Let K/k and L/k be Galois extensions of the number field k. If we have S(K/k) = S(L/k) with a possible exceptional set of Dirichlet density 0, we get K = L.

Proof.

By Proposition 2.3.2 we get [K:k] = [L:k] = [KL:k], that is K = L. \Box

According to Theorem 2.3.2, any Galois extension L/k is uniquely determined by the set S(L/k) of prime ideals that are fully decomposed in L/k. On the other hand, it is not known which sets \mathfrak{M} of prime ideals can appear as S(L/k) for some Galois extension L/k.

If we consider arbitrary extensions L/k of number fields, the set S(L/k) is not sufficient to unambiguously characterize the given extension. If N is the Galois closure of L over k, i. e. the composite of all extension fields of k conjugate to L within a fixed algebraic closure \overline{k}/k , we have S(N/k) = S(L/k). Therefore we consider instead the set

 $S_1(L/k) = \{ \mathfrak{p} | \mathfrak{p} \text{ unramified in } L/k, f_{L/k}(\mathfrak{P}) = 1 \text{ for some } \mathfrak{P} \text{ in } L \text{ over } \mathfrak{p} \}$

of all unramified prime ideals of k whose decomposition in \mathcal{O}_L contains at least one prime ideal of relative inertial degree 1. If L/k is a Galois extension, we have $S_1(L/k) = S(L/k)$.

Proposition 2.3.3.

Let L/k be any extension of number fields. Then $\delta_D(S_1(L/k)) \geq \frac{1}{[L:k]}$. Equality holds if and only if L/k is a Galois extension.

Proof.

See [Neuk92, VII. Korollar 13.5] and [Hass67, Satz (85)].

3 Elliptic Curves

This chapter contains the basic geometric facts which are required before introducing torsion point fields. The following statements are illustrated in more detail in [Silv86, III. §1,§2, App. C. §16].

Section 3.1 introduces elliptic curves and names some of their most important invariants. Section 3.2 describes the additive law of composition which exists on any elliptic curve and provides the coordinate equations derived from it. Some basic properties of those polynomials which define the coordinates of the torsion points of fixed order may be found in Section 3.3.

Sections 3.4 and 3.5 describe the structure of the group of torsion points of an elliptic curve and analyze it by means of ℓ -adic representations. For these results the reader may refer to [Silv86, III., V.] or [Serr72, §4].

The last section defines the L-series of an elliptic curve over a number field. The L-series coefficients provide additional arithmetic quantities in connection with the field extensions given by the coordinates of torsion points which are to be examined below.

3.1 Defining Equations

Let K be a perfect field, and let \overline{K} denote a separable closure of K. An *elliptic* curve E defined over K, also written E/K, is a set of homogenous coordinates (X:Y:Z) in the projective plane $\mathbb{P}^2(\overline{K})$ which satisfy an equation of the form

$$Y^{2}Z + a_{1}XYZ + a_{3}YZ^{2} = X^{3} + a_{2}X^{2}Z + a_{4}XZ^{2} + a_{6}Z^{3}$$
(3.1)

with coefficients $a_1, a_2, a_3, a_4, a_6 \in K$. The discriminant of this equation is required to be different from 0 because otherwise the respective curve has a singularity. The corresponding affine equation reads

$$y^{2} + a_{1}xy + a_{3}y = x^{3} + a_{2}x^{2} + a_{4}x + a_{6}.$$
 (3.2)

This equation is not uniquely determined with respect to the given elliptic curve E since any coordinate transformation $(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t)$ with $r, s, t \in K$ and $u \in K^*$ leads to another equation of the same shape.

C. Adelmann: LNM 1761, pp. 25–39, 2001.

[©] Springer-Verlag Berlin Heidelberg 2001

When applying this transformation, the discriminant of Equation (3.2) is multiplied by the factor u^{12} .

If the characteristic of K is not equal to 2 or 3, the affine equation is transferred by $y \mapsto y - \frac{a_1x + a_3}{2}$ and $x \mapsto x - \frac{a_1^2 + 4a_2}{12}$ into

$$y^2 = x^3 + ax + b (3.3)$$

with coefficients $a, b \in K$. This shape is only preserved by transformations $(x, y) \mapsto (u^2 x, u^3 y)$ with $u \in K^*$. Equation (3.3) possesses the discriminant

$$\Delta = -16(4a^3 + 27b^2), \tag{3.4}$$

and we require $\Delta \neq 0$. If the affine elliptic curve described by (3.2) or (3.3) is embedded by the rule $(x, y) \mapsto (x : y : 1)$ into the projective plane $\mathbb{P}^{2}(\overline{K})$ then the projective closure of this curve contains exactly one further point, namely the infinite point of the *y*-axis which has coordinates (0:1:0).

Another important quantity attached to E is its *j*-invariant

$$j = 2^6 \, 3^3 \, \frac{4a^3}{4a^3 + 27b^2}.\tag{3.5}$$

By the explanations above, each elliptic curve E can be described by different equations having different values for their respective discriminants. However, the value of j = j(E) is independent from the chosen equation. The *j*-invariant characterizes the \overline{K} -isomorphy class of E, because two elliptic curves over \overline{K} are isomorphic if and only if their *j*-invariants coincide.

3.2 Addition on Elliptic Curves

On the points of an elliptic curve we are able to define a dyadic operation which we may interpret as an addition. By means of this addition, the curve is endowed with the structure of an abelian group. The addition is performed subject to the following rule:

The sum of three points equals zero if and only if they lie on a line.

The addition is essentially given by equations describing the intersection of the curve with lines. The zero element is far away from being uniquely determined by the rule stated above. In fact, any point on E may serve as the zero element of the addition. If we choose any K-rational point to be our zero element, the addition is defined over K, i. e. the respective coordinate equations have coefficients belonging to K. Usually we select the point $\mathbf{0} = (0:1:0)$ as zero element to which we assign the formal coordinate value (∞, ∞) when we consider the affine equation (3.3). Once we fixed $\mathbf{0}$ in this way, we can describe the addition with respect to Equation (3.3) by the following relations (concerning the general case (3.1), see [Silv86, III. 2.3]).

Let P_1, P_2, P_3 be points of the curve, $P_1, P_2 \neq \mathbf{0}$, which have coordinates $P_i = (x_i, y_i)$ and satisfy the equation $P_3 = P_1 + P_2$. Then we have

$$x_{3} = \left(\frac{y_{2} - y_{1}}{x_{2} - x_{1}}\right)^{2} - x_{1} - x_{2} ,$$

$$y_{3} = -\frac{y_{2} - y_{1}}{x_{2} - x_{1}} x_{3} - \frac{y_{1}x_{2} - y_{2}x_{1}}{x_{2} - x_{1}}.$$
(3.6)

In the case $x_1 = x_2$, we have to understand this equation correctly, which means that we have to evaluate the differential quotient of (3.3). If $y_1 = -y_2$, we have $P_1 + P_2 = \mathbf{0}$, otherwise we have $P_1 = P_2$, so that we get

$$\begin{split} x_3 &= \frac{x_1^4 - 2ax_1^2 - 8bx_1 + a^2}{4(x_1^3 + ax_1 + b)}, \\ y_3 &= \frac{x_1^6 + 5ax_1^4 + 20bx_1^3 - 5a^2x_1^2 - 4abx_1 - a^3 - 8b^2}{8y_1(x_1^3 + ax_1 + b)} \end{split}$$

The set of points of an elliptic curve E becomes a \mathbb{Z} -module in the natural way by setting

$$n \cdot P = \begin{cases} \mathbf{0} & \text{for } n = 0, \\ \underbrace{P + \ldots + P}_{n-\text{times}} & \text{for } n > 0, \\ \underbrace{(-P) + \ldots + (-P)}_{|n|-\text{times}} & \text{for } n < 0. \end{cases}$$

The module E obtained in this way can be decomposed into a direct sum of a torsion module and a free module

$$E = E_{tors} \oplus E_{free} ,$$

a point P on E belonging to E_{tors} if and only if there is a $n \in \mathbb{N}$ which satisfies the equation $n \cdot P = \mathbf{0}$. Any point P of E_{tors} is called *torsion point*. The coordinates of the torsion points form the basis of the extension fields which are examined below.

3.3 Division Polynomials

We may conclude from the formulas (3.6) describing the addition of points on an elliptic curve that the coordinates of all integral multiples of a certain point are given by rational functions with coefficients from the base field in the coordinates of the respective point. This observation leads to the algebraic equations considered in this section which have to be satisfied by the coordinates of all torsion points of a fixed order.

Let E be an elliptic curve over the field K given by the equation $y^2 = x^3 + ax + b$. Then the affine coordinate ring K[E] of E is defined as

$$K[E] = K[x, y]/(y^2 - x^3 - ax - b).$$

For $m \in \mathbb{N}$ we recursively define the polynomials $A_m = A_m(x, y)$ in K[E] by

$$A_{1} = 1$$

$$A_{2} = 2y$$

$$A_{3} = 3x^{4} + 6ax^{2} + 12bx - a^{2}$$

$$A_{4} = 4y(x^{6} + 5ax^{4} + 20bx^{3} - 5a^{2}x^{2} - 4abx - 8b^{2} - a^{3})$$

$$2y A_{2m} = A_{m}(A_{m+2}A_{m-1}^{2} - A_{m-2}A_{m+1}^{2})$$

$$A_{2m+1} = A_{m+2}A_{m}^{3} - A_{m-1}A_{m+1}^{3}.$$

The index range is extended to all of \mathbb{Z} by $A_0 = 0$ and $A_{-m} = -A_m$. Using the polynomials $B_m = B_m(x, y)$ and $C_m = C_m(x, y)$ in K[E] given by

$$B_m = xA_m^2 - A_{m-1}A_{m+1}$$

4y C_m = A_{m+2}A_{m-1}² - A_{m-2}A_{m+1}²

the coordinates of the *m*-fold of the point (x, y) of E satisfy the equality

$$m \cdot (x, y) = \left(\frac{B_m(x, y)}{A_m(x, y)^2}, \frac{C_m(x, y)}{A_m(x, y)^3}\right).$$
(3.7)

The polynomials A_m, B_m, C_m are called *division polynomials*, this notion frequently being used only for the polynomials A_m . In the above form, A_m, B_m, C_m can be viewed as polynomials from $\mathbb{Z}[x, y, a, b]/(y^2 - x^3 - ax - b)$, from which we may get to elements of K[E] by specializing the parameters a and b. The polynomials A_m, B_m, C_m possess uniquely determined representatives in $\mathbb{Z}[x, y, a, b]$, if we require of y to appear in every monomial at most to the first power. Subject to the same condition we also find for any special value of a, b exactly one representative of each respective polynomial in K[x, y] over K[E]. All these polynomials which are uniquely determined by the above conditions are denoted by A_m, B_m, C_m . The division polynomials have the following properties (cf. [Lang78]):

- The polynomials A_{2m+1}, B_m, C_{2m} are elements of Z[x, a, b], as well as the polynomials y⁻¹A_{2m} and y⁻¹C_{2m+1}. Therefore, A²_m, B_m, C²_m are polynomials in Z[x, a, b].
- 2. If we assign weights to the variables in $\mathbb{Z}[x, y, a, b]$, namely

to x the weight 2,	to a the weight 4,
to y the weight 3,	to b the weight 6.

then the polynomials A_m, B_m, C_m are homogenous with respect to these weights. They have the weights $m^2 - 1$, $2m^2$, $3m^2$, respectively.

3. The polynomials A_m^2 and B_m in $\mathbb{Z}[a, b, x]$ satisfy the relations

$$A_{mn}^{2}(x) = A_{n}^{2m^{2}}(x) A_{m}^{2} \left(\frac{B_{n}(x)}{A_{n}^{2}(x)}\right),$$
$$B_{mn}(x) = A_{n}^{2m^{2}}(x) B_{m} \left(\frac{B_{n}(x)}{A_{n}^{2}(x)}\right).$$

Particularly, we conclude from the first equation that $A_m^2(x)$ is a divisor of $A_n^2(x)$ if m is a divisor of n.

4. If 2^k is the highest power of 2 dividing m, the greatest common divisor of the coefficients of A_m^2 is equal to 2^{2k} . Especially, the greatest common divisor of the coefficients of A_{2m+1}^2 is equal to 1 since we have

$$A_{2m+1}(0, y, a, 0) = (-1)^m a^{m^2 + m}$$

- 5. If p is a prime number and s a natural number then the quotient $\Lambda_{p^s} = A_{p^s}/A_{p^{s-1}}$ is again a polynomial from $\mathbb{Z}[x, a, b]$ having the highest coefficient p.
- 6. The polynomials A_m^2 and B_m are relatively prime to each other. In particular, we have

$$(3x^3 - 5ax - 27b)A_2^2 - (12x^2 + 16a)B_2 = -4(4a^3 + 27b^2)$$

7. The absolute value of the coefficients of the polynomials A_m^2 and B_m from $\mathbb{Z}[x, a, b]$ can be bounded by C^{m^2} with a constant C > 1 whose value only depends on a and b (see also [McKe94, Cor. 1]).

3.4 Torsion Points

Let *E* be an elliptic curve given by the equation $y^2 = x^3 + ax + b$ which is defined over the perfect field *K*. By Section 3.2 the rule $P \mapsto n \cdot P$ provides for each $n \in \mathbb{Z}$ an endomorphism $[n] : E \to E$ defined over *K*. These endomorphisms are distinct over a separable closure \overline{K} (cf. [Silv86, III. 4.2]) such that we have a ring monomorphism $\mathbb{Z} \to \text{End}(E)$, $n \mapsto [n]$.

For $n \in \mathbb{N}$, let E_n denote the set of *n*-torsion points of E,

$$E_n = \ker ([n] : E \to E) = \{ P \in E \mid n \cdot P = \mathbf{0} \}.$$

Since the multiplication map [n] is compatible with the addition, the set E_n is a submodule of the module E_{tors} of all torsion points of E. The annihilator of the \mathbb{Z} -module E_n is equal to the ideal $n\mathbb{Z}$. Hence, E_n is a faithful $\mathbb{Z}/n\mathbb{Z}$ -module. The structure of this module is described by the following proposition.

Proposition 3.4.1.

- (a) For $m, n \in \mathbb{N}$ satisfying (m, n) = 1, we have $E_{mn} \cong E_m \times E_n$.
- (b) If $n \in \mathbb{N}$ is prime to the characteristic of K, we have

$$E_n \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

(c) If the characteristic of K is equal to p > 0, we have either $E_{p^m} = \{\mathbf{0}\}$ for all $m \in \mathbb{N}$ or $E_{p^m} \cong \mathbb{Z}/p^m\mathbb{Z}$ for all $m \in \mathbb{N}$.

Proof.

In (a) the map $E_m \times E_n \to E_{mn}$, $(P,Q) \mapsto P+Q$, provides an isomorphism of **Z**-modules. (b) and (c) see [Silv86, III. 6.4].

Corollary 3.4.1.

For (m, n) = 1 we have $\operatorname{Aut}(E_{mn}) \cong \operatorname{Aut}(E_m) \times \operatorname{Aut}(E_n)$.

Proof.

The statement may be concluded directly from Proposition 3.4.1 (a), similar to [Hupp67, I. 9.4]. $\hfill \Box$

We intend to investigate for all $n \in \mathbb{N}$ the fields

$$K(E_n) = K(x, y \mid (x, y) \in E_n) = K(x, y \mid (x, y) \in E, n \cdot (x, y) = \mathbf{0})$$

which are formed by adjoining to K the coordinates of all *n*-torsion points of E. $K(E_n)$ is called the *n*-th *torsion point field*, and the extension $K(E_n)/K$ is called the *n*-th *torsion point extension*.
One important subextension of $K(E_n)/K$ is generated by the x-coordinates of the points in E_n ,

$$K(x(E_n)) = K(x \mid (x, y) \in E_n).$$

The absolute Galois group $\operatorname{Gal}(\overline{K}/K)$ operates on the elliptic curve E by applying its \overline{K} -automorphisms to the coordinates of the points of E. Since the addition on E and the coordinates of the points in E_n are given by algebraic equations with coefficients from K (see (3.6) and (3.7)), this Galois operation is compatible with the addition on E and consequently with the multiplication [n] such that n-torsion points are again mapped to n-torsion points. In this way $\operatorname{Gal}(\overline{K}/K)$ also operates on E_n , and we get a representation

$$\varphi_n : \operatorname{Gal}(\overline{K}/K) \to \operatorname{Aut}(E_n),$$

where $\operatorname{Aut}(E_n)$ denotes the ring of module automorphisms of E_n . This representation is continuous with respect to the Krull topology of profinite groups because its image is finite, hence its kernel is a normal subgroup of finite index in $\operatorname{Gal}(\overline{K}/K)$.

The fixed field corresponding to $\ker(\varphi_n)$ is equal to $K(E_n)$, since on the one hand, the operation of $\ker(\varphi_n)$ on E_n and hence on $K(E_n)$ is trivial, and on the other hand, any automorphism of \overline{K} which fixes each element of $K(E_n)$ induces the identity on E_n . In particular, $K(E_n)/K$ is a Galois extension, and φ_n factorizes via $\operatorname{Gal}(K(E_n)/K)$ to give a faithful representation

$$\overline{\varphi}_n : \operatorname{Gal}(K(E_n)/K) \to \operatorname{Aut}(E_n) .$$
 (3.8)

If n is prime to the characteristic of K then by Proposition 3.4.1 (b), E_n is a faithful $\mathbb{Z}/n\mathbb{Z}$ -module of rank 2, having an automorphism group isomorphic to

$$\operatorname{GL}(2,n) = \operatorname{GL}(2, \mathbb{Z}/n\mathbb{Z}) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in \mathbb{Z}/n\mathbb{Z}, (ad-bc, n) = 1 \}, \quad (3.9)$$

where the correspondence between the module automorphisms and the matrices includes the selection of some $\mathbb{Z}/n\mathbb{Z}$ -module basis $\{P, Q\}$ of E_n . The module automorphism belonging to $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is then described by the mapping $P \mapsto aP + cQ$, $Q \mapsto bP + dQ$ of the basis elements.

If K has characteristic p > 0 and p is a divisor of n, the description of $K(E_n)$ can be reduced, by Proposition 3.4.1 (a), to already treated cases and to the cases of prime powers p^m . In the latter cases, depending on Proposition 3.4.1 (c), we get faithful representations which are either of the form $\overline{\varphi}_{p^m}$: $\operatorname{Gal}(K(E_{p^m})/K) \to (\mathbb{Z}/p^m\mathbb{Z})^*$ or of the form $\overline{\varphi}_{p^m}$: $\operatorname{Gal}(K(E_{p^m})/K) \to 1$.

Hence, if the characteristic of K is no divisor of n, we may view the Galois group of the *n*-th torsion point extension as a subgroup of GL(2, n), due to the injectivity of $\overline{\varphi}_n$. The surjectivity of φ_n is treated in the following section.

3.5 ℓ -adic Representations

Let K be a perfect field, and let E be an elliptic curve defined over K. By the elucidations of the preceding section, the operation of the absolute Galois group $\operatorname{Gal}(\overline{K}/K)$ on E_n provides a continuous representation

$$\varphi_n : \operatorname{Gal}(\overline{K}/K) \to \operatorname{Aut}(E_n)$$

When examining the image of φ_n we may by Corollary 3.4.1 restrict ourselves to torsion points of fixed order which is the power of a prime number.

In this section let ℓ always denote a prime number. We intend to consider the set $E_{\ell^{\infty}}$ formed as the union of all torsion points of E whose order is some power of ℓ . We also look at the ℓ -adic *Tate-module*

$$T_{\ell}(E) = \lim_{\longleftarrow \atop m} E_{\ell^m} ,$$

the projective limit being formed with respect to the multiplication $[\ell]$. This construction is in a certain sense dual to $E_{\ell^{\infty}}$. Both $E_{\ell^{\infty}}$ and $T_{\ell}(E)$ own a natural structure as a \mathbb{Z}_{ℓ} -module.

If ℓ is not equal to the characteristic of K, we conclude from Proposition 3.4.1 (b) that $T_{\ell}(E)$ is isomorphic to $(\mathbb{Z}_{\ell})^2$, i. e. $T_{\ell}(E)$ is a free \mathbb{Z}_{ℓ} -module of rank 2. On the other hand, $E_{\ell^{\infty}}$ proves to be isomorphic to $(\mathbb{Q}_{\ell}/\mathbb{Z}_{\ell})^2$ which cannot be given the structure of a free \mathbb{Z}_{ℓ} -module. Therefore, we prefer to consider $T_{\ell}(E)$. If we endow the finite sets E_{ℓ^m} with the discrete topology, the topology given by the limit process on $T_{\ell}(E)$ coincides with the ℓ -adic topology defined on it as the product topology of copies of \mathbb{Z}_{ℓ} .

Each endomorphism of E gives rise to an endomorphism of $T_{\ell}(E)$ by restricting it to the ℓ -power torsion points. In this way we get a representation

$$r_{\ell} : \operatorname{End} E \to \operatorname{End} T_{\ell}(E) , \qquad (3.10)$$

which is called the ℓ -adic representation of the endomorphism ring of E. End $T_{\ell}(E)$ is isomorphic to $M(2, \mathbb{Z}_{\ell})$, the ring of 2×2 -matrices with entries from \mathbb{Z}_{ℓ} , where assigning a module endomorphism to a matrix requires the prior selection of a \mathbb{Z}_{ℓ} -module basis of $T_{\ell}(E)$. The matrices which may be assigned to a given module endomorphism ϕ_{ℓ} in End $T_{\ell}(E)$, however, all lie within the same similarity class. The characteristic polynomial of ϕ_{ℓ} is therefore unambiguously defined in $\mathbb{Z}_{\ell}[X]$, no matter which specific basis is considered. Consequently, quantities like the trace and the determinant of ϕ_{ℓ} are well-defined.

Let now the base field K of the elliptic curve E be the finite field \mathbb{F}_q which has q elements and is of characteristic p. The Frobenius automorphism

$$\pi_q: \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q \\ x \mapsto x^q$$

provides an endomorphism $\pi_q: E \to E$ by application to the coordinates of the points of E. The characteristic polynomial of $r_{\ell}(\pi_q)$ is for $\ell \neq p$ equal to

$$\det(X - r_{\ell}(\pi_q)) = X^2 - a_q X + q.$$
(3.11)

This assertion is concluded by the existence of a non-degenerate, alternating bilinear form on $T_{\ell}(E)$ (see [Silv86, V. §2, p. 135f.]). The coefficient a_q in (3.11) is given by

$$a_q = q + 1 - \# E(\mathbf{F}_q) , \qquad (3.12)$$

if $#E(\mathbb{F}_q)$ denotes the number of \mathbb{F}_q -rational points of E.

By (3.11), a_q is equal to the trace of $r_{\ell}(\pi_q)$, i. e. equal to the trace of the ℓ -adic representation of the Frobenius endomorphism π_q , and the values of these traces coincide for all prime numbers $\ell \neq p$.

Similarly, if K is any perfect field, the operation of the absolute Galois group of K via φ_{ℓ^m} leads to a representation

$$\varrho_{\ell} : \operatorname{Gal}(\overline{K}/K) \to \operatorname{Aut}(T_{\ell}(E)),$$

called the ℓ -adic representation of $\operatorname{Gal}(\overline{K}/K)$, and the image of ϱ_{ℓ} contains only continuous automorphisms of $T_{\ell}(E)$. If ℓ is not equal to the characteristic of K, $\operatorname{Aut}(T_{\ell}(E))$ is isomorphic to

$$\operatorname{GL}(2, \mathbb{Z}_{\ell}) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}_{\ell} , ad - bc \neq 0 \}.$$

If the base field K of the elliptic curve E is an algebraic number field k then there is an intimate connection between r_{ℓ} and ϱ_{ℓ} which enables us to use the geometric quantity a_q to describe Galois theoretic properties of the torsion point extensions. This relation is explained in greater detail in the following section.

Concerning the surjectivity of the representations defined above, we have the following results.

Proposition 3.5.1. (Serre)

Let k be an algebraic number field. Then the following statements are equivalent:

- (a) $\varrho_{\ell} : \operatorname{Gal}(\overline{k}/k) \to \operatorname{Aut}(T_{\ell}(E))$ is surjective for all up to finitely many prime numbers ℓ .
- (b) $\varphi_{\ell} : \operatorname{Gal}(k/k) \to \operatorname{Aut}(E_{\ell})$ is surjective for all up to finitely many prime numbers ℓ .

Proof. See [Serr68, p. IV-19]. If the elliptic curve E has strictly more endomorphisms defined over k than those given by the maps $[n]: E \to E$, we say, E has *complex multiplication* over k.

Proposition 3.5.2. (Serre)

If the elliptic curve E has no complex multiplication over k, we have:

- (a) The index of $\varphi_n(\operatorname{Gal}(\overline{k}/k))$ in $\operatorname{Aut}(E_n)$ is bounded from above by a constant whose value only depends on E and k.
- (b) The representation φ_{p^m} : $\operatorname{Gal}(\overline{k}/k) \to \operatorname{Aut}(E_{p^m})$ is surjective for all up to finitely many prime numbers p.

Proof.

See [Serr72, p. 259-260].

If the elliptic curve E has complex multiplication over k, however, the image of φ_n is always an abelian group [Silv86, III. 7.10], hence φ_n is not surjective for all $n \geq 2$.

If E is an elliptic curve defined over k having complex multiplication over k, all endomorphisms of E are already defined over an imaginary quadratic extension of k (see [Shim71, (5.1.3)]), and the images of φ_n are either abelian groups or generalized dihedral groups, i. e. semidirect products of abelian groups by $\mathbb{Z}/2\mathbb{Z}$.

We may conclude from Proposition 3.5.2 that, given k and E, there is a constant c = c(E, k) such that φ_{ℓ} is surjective for all prime numbers ℓ satisfying $\ell \geq c$. If the base field is $k = \mathbb{Q}$, we have the following result in this direction.

Proposition 3.5.3.

Let E be a semistable elliptic curve defined over \mathbb{Q} without complex multiplication. Then we have $\varphi_{\ell}(\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \operatorname{Aut}(E_{\ell})$ for all prime numbers $\ell \geq 11$.

Proof.

See [Rath88, 5.4]. The result is based on the determination of E_{tors} in [Mazu78].

3.6 Reduction Modulo **p** and L-Series

Let k be a number field and E an elliptic curve defined over k. We establish a connection between locally and globally defined structures related to E. At first we describe the principle of reducing E modulo a prime ideal \mathfrak{p} .

Within the entire following section, let \mathfrak{p} denote a prime ideal of \mathcal{O}_k different from $\{0\}$ which has the absolute norm $q = N(\mathfrak{p})$. By reducing a defining equation of the form (3.1) of E modulo \mathfrak{p} we get the equation of a curve \tilde{E} defined over the residue field $\kappa(\mathfrak{p}) = \mathcal{O}_k/\mathfrak{p}$. This curve, however, may possess singularities if the discriminant is reduced to 0. If we find a description of E by an equation of the form (3.1) whose reduction modulo \mathfrak{p} defines a non-singular curve \tilde{E} , \tilde{E} is again an elliptic curve. In this case we say, E has good reduction at \mathfrak{p} , otherwise E has bad reduction at \mathfrak{p} . Bad reduction appears for at most finitely many \mathfrak{p} .

Elliptic curves only have a few types of bad reduction. On any reduced curve there is no more than one singular point over $\overline{\kappa(\mathbf{p})}$. For such a point P there are two geometrically different cases to be considered:

- -P is a knot, i. e. there are two different tangents to the curve in P. In this case we say, E has *multiplicative reduction* with respect to \mathfrak{p} . If the tangent slopes are values in the base field k, we talk of *split multiplicative reduction* with respect to \mathfrak{p} .
- -P is a cusp, i. e. there is only one tangent to the curve E in P. Then E has *additive reduction* with respect to \mathfrak{p} .

If an elliptic curve has good or multiplicative reduction at all prime ideals, the curve is called *semistable*.

One important combinatorial quantity which contributes to our local data is for any given \mathfrak{p} the number of points of \tilde{E} which are defined over the residue field $\kappa(\mathfrak{p}) \cong \mathbb{F}_q$ and its finite extensions \mathbb{F}_{q^n} , respectively. We define for $n \in \mathbb{N}$ the numbers $a_{q^n} \in \mathbb{Z}$ by

$$a_{q^n} = q^n + 1 - \#\tilde{E}(\mathbb{F}_{q^n}). \tag{3.13}$$

 a_{q^n} measures the difference of the number of \mathbb{F}_{q^n} -rational points of \tilde{E} from their average value $q^n + 1$. Some basic properties of a_{q^n} are summarized in the following proposition.

Proposition 3.6.1.

If $\mathfrak{p} \neq \{0\}$ is a prime ideal of \mathcal{O}_k having the norm $q = N(\mathfrak{p})$, the quantities a_{q^n} of (3.13) satisfy:

(a) If E has good reduction at \mathfrak{p} , we have the formulas

$$a_{q^{n+1}} = a_q \, a_{q^n} - q \, a_{q^{n-1}} \quad \text{for } n \ge 2,$$

 $a_{q^2} = a_q^2 - 2 \, q.$

(b) If E has bad reduction at \mathfrak{p} , we have for $n \in \mathbb{N}$

$$a_{q^n} = \begin{cases} 1 & \text{in the case of split multiplicative reduction mod } \mathfrak{p}, \\ (-1)^n & \text{in the case of non-split multiplicative reduction mod } \mathfrak{p}, \\ 0 & \text{in the case of additive reduction mod } \mathfrak{p}. \end{cases}$$

Proof.

(a) see [Silv86, V. §2, p. 136]. (b) see [Silv86, III. 2.5, 2.6, ex. 3.5]. □

We especially notice that all quantities a_{q^n} with $n \in \mathbb{N}$ are uniquely determined as soon as a_q is known. a_q has already appeared in Section 3.5 (see (3.12)) in connection to the Frobenius endomorphism π_q on \tilde{E} . We now relate it to globally defined structures.

Let \mathfrak{p} be a prime ideal of k with the norm q such that E has good reduction at \mathfrak{p} , and let ℓ be some prime number not divided by \mathfrak{p} . The process of reduction modulo \mathfrak{p} provides group homomorphisms $E_{\ell^n} \to \tilde{E}_{\ell^n}$ which prove to be isomorphisms under our assumptions to \mathfrak{p} and ℓ , injectivity being the most difficult assertion (see [Silv86, VII 3.1(b)]). Hence the ℓ -adic Tate-modules $T_{\ell}(E)$ and $T_{\ell}(\tilde{E})$ are isomorphic, and by conjugation with some such isomorphism we get a representation

$$\tilde{\varrho}_{\ell} : \operatorname{Gal}(\overline{k}/k) \to \operatorname{Aut} T_{\ell}(E) \to \operatorname{Aut} T_{\ell}(\tilde{E})$$
.

If K_{ℓ} is the fixed field in \overline{k} corresponding to ker $(\tilde{\varrho}_{\ell})$, \mathfrak{p} is unramified in K_{ℓ}/k . Let $\sigma_{\mathfrak{p}}$ be some element of $\operatorname{Gal}(\overline{k}/k)$ whose restriction to K_{ℓ} is equal to the Frobenius element of some prime of K_{ℓ} lying over \mathfrak{p} . If the isomorphism $T_{\ell}(E) \to T_{\ell}(\tilde{E})$ is properly chosen, we have $\tilde{\varrho}_{\ell}(\sigma_{\mathfrak{p}}) = r_{\ell}(\pi_q)$, see [Shim71, 7.6], in any case the characteristic polynomial of $\tilde{\varrho}_{\ell}(\sigma_{\mathfrak{p}})$ is by (3.11) equal to

$$\det(X - \tilde{\varrho}_{\ell}(\sigma_{\mathfrak{p}})) = X^2 - a_q X + q.$$

On the other hand, $\tilde{\varrho}_\ell$ may be constructed via projective limit from representations

$$\tilde{\varphi}_{\ell^m} : \operatorname{Gal}(\overline{k}/k) \to \operatorname{Aut} E_{\ell^m} \to \operatorname{Aut} \tilde{E}_{\ell^m}.$$

By Section 3.4 the fixed field of $\ker(\tilde{\varphi}_{\ell^m})$ is equal to $k(E_{\ell^m})$. Since $k(E_{\ell^m})$ is a subfield of K_{ℓ} , \mathfrak{p} is unramified in $k(E_{\ell^m})/k$, and the restriction of $\sigma_{\mathfrak{p}}$ to $k(E_{\ell^m})$ is the Frobenius element of some prime ideal in $k(E_{\ell^m})$ lying over \mathfrak{p} .

Aut \tilde{E}_{ℓ^m} is isomorphic to $\operatorname{GL}(2, \ell^m)$, therefore the characteristic polynomial of $\tilde{\varphi}_{\ell^m}(\sigma_{\mathfrak{p}})$ in $(\mathbb{Z}/\ell^m\mathbb{Z})[X]$ is given by

$$\det(X - \tilde{\varphi}_{\ell^m}(\sigma_{\mathfrak{p}})) = X^2 - a_q X + q,$$

and this equality holds for every Frobenius element $\sigma_{\mathfrak{p}}$ chosen as above. In particular, the trace of $\tilde{\varphi}_{\ell^m}(\sigma_{\mathfrak{p}})$ satisfies

$$\operatorname{Tr}(\tilde{\varphi}_{\ell^m}(\sigma_{\mathfrak{p}})) \equiv a_q \mod \ell^m . \tag{3.14}$$

Thus, if we restrict our attention to $k(E_{\ell^m})$, a_q coincides modulo ℓ^m with the trace of the ℓ -adic representation of any Frobenius element attached to \mathfrak{p} . However, since $\tilde{\varphi}_{\ell^m}$ is not a representation in characteristic 0 we are not able to recover the conjugacy class of the Frobenius elements belonging to \mathfrak{p} if we are only given the knowledge of $a_q \mod \ell^m$.

So far, we have used the global operation of the absolute Galois group of k to obtain local quantities which count those points on the reduced curve \tilde{E} which are rational over the respective residue field. Now we go the other way and construct a global structure on E by combining the local quantities a_q with respect to the reductions of E modulo all prime ideals \mathfrak{p} of k. We arrive at the definition of a complex valued function called the L-series of the elliptic curve E.

For any prime ideal \mathfrak{p} of k, the \mathfrak{p} -adic zeta function of \tilde{E} over $\kappa(\mathfrak{p})$ is given by

$$Z(\tilde{E}/\kappa(\mathfrak{p}),T) = \exp\left(\sum_{n=1}^{\infty} \#(\tilde{E}(\kappa_n(\mathfrak{p}))) \frac{T^n}{n}\right),$$

where $\kappa_n(\mathfrak{p})$ denotes the extension of $\kappa(\mathfrak{p})$ of degree *n* which is uniquely determined up to field isomorphisms.

Proposition 3.6.2.

Let $\mathfrak{p} \neq \{0\}$ be a prime ideal of \mathcal{O}_k having the norm $q = N(\mathfrak{p})$ such that E has good reduction at \mathfrak{p} . Then the \mathfrak{p} -adic zeta function has the following properties:

(a) It is a rational function in $\mathbb{Q}(T)$. More precisely, we have

$$Z(\tilde{E}/\kappa(\mathfrak{p}),T) = \frac{1-a_qT+qT^2}{(1-T)(1-qT)}.$$

(b) It satisfies the functional equation

$$Z(\tilde{E}/\kappa(\mathfrak{p}),\frac{1}{qT})=Z(\tilde{E}/\kappa(\mathfrak{p}),T).$$

(c) The numerator polynomial in (a) has the following decomposition in $\mathbb{C}[T]$

$$1 - a_q T + q T^2 = (1 - \alpha T)(1 - \overline{\alpha} T) \quad with \quad |\alpha| = \sqrt{q}.$$

Proof.

These statements are a special case of the Weil conjectures on zeta functions of smooth projective varieties. See [Silv86, V. 2.4]. □

By Proposition 3.6.2 we are able to estimate the size of a_{q^n} .

Corollary 3.6.1.

If $\mathfrak{p} \neq \{0\}$ is a prime ideal of \mathcal{O}_k having the norm $q = N(\mathfrak{p})$ such that E has good reduction at \mathfrak{p} , the numbers a_{q^n} satisfy the inequality

$$|a_{q^n}| \le 2\sqrt{q^n}.$$

Proof.

This assertion may be concluded from Proposition 3.6.2 (c), and the expression $a_{q^n} = \alpha^n + \overline{\alpha}^n$.

For any prime ideal \mathfrak{p} having the norm q we define the local factor $L_{\mathfrak{p}}(T)$ with respect to \mathfrak{p} of the L-series of E by

 $L_{\mathfrak{p}}(T) = \begin{cases} 1 - a_q T + q T^2, & \text{if } E \text{ has good reduction at } \mathfrak{p}, \\ 1 - T, & \text{if } E \text{ has split multiplicative reduction at } \mathfrak{p}, \\ 1 + T, & \text{if } E \text{ has non-split multiplicative reduction at } \mathfrak{p}, \\ 1, & \text{if } E \text{ has additive reduction at } \mathfrak{p}. \end{cases}$ (3.15)

For all types of reduction the following formula holds:

$$L_{\mathfrak{p}}((N(\mathfrak{p}))^{-1}) = \frac{\#(\tilde{E}_{ns}(\kappa(\mathfrak{p})))}{N(\mathfrak{p})}$$

where $\#(\tilde{E}_{ns}(\kappa(\mathfrak{p})))$ denotes the number of non-singular, $\kappa(\mathfrak{p})$ -rational points of the curve \tilde{E} reduced modulo \mathfrak{p} . In terms of these factors we define the *L*-series of the elliptic curve E over k as a function in the complex variable s,

$$L_{E/k}(s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(N(\mathfrak{p})^{-s})^{-1}.$$
 (3.16)

By Proposition 3.6.2 (c), the product is convergent for all complex s with $\operatorname{Re}(s) > \frac{3}{2}$, and in this domain it converges absolutely and uniformly on compact subsets and hence represents a holomorphic function in s.

If we write the L-series of E as a Dirichlet series in the form

$$L_{E/k}(s) = \sum_{n=1}^{\infty} c_n n^{-s},$$

the coefficients c_n have, due to the product expression (3.16), the following properties:

- 1. They are integral and multiplicative, i. e. for all indices $m, n \in \mathbb{N}$ satisfying (m, n) = 1 we have $c_{mn} = c_m c_n$.
- 2. For each prime ideal \mathfrak{p} of the norm q with good reduction we have

$$c_{q^{n+1}} = c_q c_{q^n} - q c_{q^{n-1}}$$
 for $n \ge 2$,
 $c_{q^2} = c_q^2 - q$.

3. For each prime ideal \mathfrak{p} of the norm q with bad reduction we have

$$c_{q^n} = \begin{cases} 1 & \text{in the case of split multiplicative reduction mod } \mathfrak{p}, \\ (-1)^n & \text{in the case of non-split multiplicative reduction mod } \mathfrak{p}, \\ 0 & \text{in the case of additive reduction mod } \mathfrak{p}. \end{cases}$$

We notice the similarity of these formulas to those listed in Proposition 3.6.1, but we emphasize the difference between the expressions for a_{q^2} and c_{q^2} .

If E has good reduction at the prime ideal \mathfrak{p} of k with the norm q, the L-series coefficient c_q coincides with a_q as defined in (3.12). Therefore, we might have defined the local factor $L_{\mathfrak{p}}(T)$ of the L-series in terms of the ℓ -adic representation $r_{\ell}(\pi_q)$ of the Frobenius endomorphism of \tilde{E} , or, alternatively, by the ℓ -adic representation $\tilde{\varrho}_{\ell}(\sigma_{\mathfrak{p}})$ of some Frobenius element belonging to \mathfrak{p} , similar to the definition of the local factors of some Artin L-series.

As we now know the equality $c_q = a_q$, we are also able to estimate the size of the L-series coefficients c_n by means of Proposition 3.6.2.

Corollary 3.6.2.

If \mathfrak{p} is a prime ideal of k with the norm q, we have the inequality

$$|c_{q^n}| \le (n+1)\sqrt{q^n}$$

Proof.

If *E* has good reduction at \mathfrak{p} , we deduce the desired result by means of Proposition 3.6.2 (c), using the expression $c_{q^n} = \sum_{i=0}^n \alpha^i \overline{\alpha}^{n-i}$. If *E* has bad reduction at \mathfrak{p} , the estimate is obvious.

If the base field is equal to \mathbb{C} and E is an elliptic modular curve $X_0(N)$, the coefficient a_p , whose index is a prime number p satisfying p/N, also appears as eigenvalue of the p-th Hecke operator on the space of cusp forms of weight 2 with respect to the congruence subgroup $\Gamma_0(N)$ of $\mathrm{SL}(2, \mathbb{Z})$. Moreover, we are able to show that the modular curves $X_0(N)$ may be defined over \mathbb{Q} such that we get a connection between the operation of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $X_0(N)$ and the operation of Hecke operators on certain spaces of meromorphic functions related to $X_0(N)$. This connection is explained in more detail within the next chapter.

4 Elliptic Modular Curves

In this chapter we elucidate the basic facts which lead to the Eichler-Shimura formula, and we explain its arithmetical importance. Within this monograph, we can only outline the far-reaching connections. More detailed information may for example be found in [Shim71], [SwBi75] and [Knap92].

In the first section, we define the operation of subgroups of $SL(2, \mathbb{Z})$ on the extended complex upper half plane and interpret the resulting quotient spaces as Riemann surfaces and algebraic curves over \mathbb{C} .

The second section touches the theory of modular forms, i. e. of differential forms on these curves. The structure of the corresponding function spaces is uncovered by means of Hecke operators.

Finally we state the Eichler-Shimura formula which provides a link between eigenvalues of suitable Hecke operators and L-series of elliptic curves. As a conclusion, we get in the case of elliptic modular curves a coincidence between certain L-series coefficients and eigenvalues of appropriate Hecke operators.

4.1 Modular Curves

Let $\mathfrak{H}=\{\,\tau\in\mathbb{C}\mid {\rm Im}(\tau)>0\,\,\}$ be the upper half plane of the complex plane. The linear group

$$\operatorname{GL}(2,\mathbb{R})_{+} = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \mid a, b, c, d \in \mathbb{R} , \ ad - bc > 0 \right\}$$
(4.1)

operates on \mathfrak{H} by mapping each matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to the rational transformation $t_A : \mathfrak{H} \to \mathfrak{H}, \tau \mapsto \frac{a\tau+b}{c\tau+d}$. Let G be a subgroup of $\mathrm{GL}(2,\mathbb{R})_+$. Two elements $\tau, \tau' \in \mathfrak{H}$ are called

Let G be a subgroup of $\operatorname{GL}(2, \mathbb{R})_+$. Two elements $\tau, \tau' \in \mathfrak{H}$ are called *G*-equivalent if there is an $A \in G$ satisfying $A(\tau) = \tau'$. This rule defines an equivalence relation on \mathfrak{H} whose equivalence classes are called *orbits*. The set of all orbits in \mathfrak{H} under the operation of G is named the quotient set $G \setminus \mathfrak{H}$.

The quotients $G \setminus \mathfrak{H}$ are to be interpreted as curves over \mathbb{C} . If we want $G \setminus \mathfrak{H}$ to have a sufficiently good structure, for example to be a locally compact Hausdorff space, we have to restrict ourselves to certain discrete subgroups of $\mathrm{GL}(2,\mathbb{R})_+$, and we must possibly extend the domain of operation \mathfrak{H} by additional points. This topic is studied in greater detail in [Shim71, chap. 1].

[©] Springer-Verlag Berlin Heidelberg 2001

In the sequel we only consider subgroups Γ of finite index in $\mathrm{SL}(2, \mathbb{Z})$. The kernel of the operation of $\mathrm{SL}(2, \mathbb{Z})$ on \mathfrak{H} is equal to $\{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$. If we examine the transformations induced by Γ on \mathfrak{H} , we consider instead of Γ the subgroup $\overline{\Gamma} = \Gamma \cdot \{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}/\{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$ of $\mathrm{PSL}(2, \mathbb{Z}) = \mathrm{SL}(2, \mathbb{Z})/\{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$ whose operation is faithful.

If we extend \mathfrak{H} by the rational points of the real axis and by the point ∞ , viewed as infinite point of the positive imaginary axis, i. e. we form

$$\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\} = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q}),$$

we may extend the operation of $SL(2, \mathbb{Z})$ to \mathfrak{H}^* . The points of $\mathbb{Q} \cup \{\infty\}$ are called *cusps*.

For $t \in \mathfrak{H}^*$ let $\Gamma_t = \{\gamma \in \Gamma \mid \gamma(t) = t\}$ denote the stabilizer subgroup of t. $\tau \in \mathfrak{H}$ is called *elliptic point* if we have $\Gamma_{\tau} \neq \{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$, that is, if τ is a fixed point of a non-trivial transformation on \mathfrak{H} .

Let $X_{\Gamma} = \Gamma \setminus \mathfrak{H}^*$ be the set of orbits of Γ in \mathfrak{H}^* . Since Γ transforms cusps into cusps and elliptic points into elliptic points, we can transfer these two notions to X_{Γ} .

If we endow \mathfrak{H}^* with the metric topology induced from $\mathbb{P}^1(\mathbb{C})$, the quotient topology given on X_{Γ} is not Hausdorff. The metric topology has to be refined at the cusps so that each cusp becomes equivalent to the point ∞ . For each cusp s, we let a fundamental basis of open sets consist of the sets $U_{\varepsilon}(s)$ for all $\varepsilon > 0$, where

$$U_{\varepsilon}(s) = \{\tau \in \mathfrak{H} \mid |\tau - s - i\varepsilon| < \varepsilon\} \cup \{s\} \text{ for } s \in \mathbb{Q}, \\ U_{\varepsilon}(\infty) = \{\tau \in \mathfrak{H} \mid \operatorname{Im}(\tau) > \varepsilon\} \cup \{\infty\}.$$

The quotient topology induced by this topology of \mathfrak{H}^* lets X_{Γ} become a compact Hausdorff space.

 X_{Γ} becomes a *Riemann surface* by assigning a complex structure to it. The complex structure is determined by holomorphically compatible *cards* (U_t, p_t) for $t \in X_{\Gamma}$ which have the following properties:

- 1. U_t is an open neighbourhood of t in X_{Γ} ,
- 2. $p_t: U_t \to \mathbb{C}$ is a homeomorphism onto an open subset of \mathbb{C} ,
- 3. for $t, t' \in \Gamma \setminus \mathfrak{H}^*$ the map $p_{t'} \circ p_t^{-1} : p_t(U_t \cap U_{t'}) \to p_{t'}(U_t \cap U_{t'})$ is biholomorphic.

We only need enough cards to cover X_{Γ} by open sets U_t . The cards are obtained as follows (cf. [Shim71, 1.5]). Let $\pi : \mathfrak{H}^* \to X_{\Gamma}$ denote the projection. For $t \in \mathfrak{H}^*$, let V_t be an open neighbourhood of t which is sufficiently small to contain as few Γ -equivalent points as possible, i. e. we require from each $\gamma \in \Gamma$

$$\gamma(V_t) \cap V_t \neq \emptyset \implies \gamma \in \Gamma_t.$$

Then the canonical map $\Gamma_t \setminus V_t \to \Gamma \setminus \mathfrak{H}^*$ is injective, and $\Gamma_t \setminus V_t$ is an open neighbourhood of $\pi(t)$ in X_{Γ} .

The requested cards have the shape $(\Gamma_t \setminus V_t, p_t)$ where p_t is one of the following maps:

- Let $\tau \in \mathfrak{H}$ satisfy $|\overline{\Gamma_{\tau}}| = n$. Let $\varphi : \mathfrak{H} \to \mathcal{E}$ be a biholomorphic mapping into the open unit disc \mathcal{E} with $\varphi(\tau) = 0$, for example $\varphi(z) = \frac{z-\tau}{z-\overline{\tau}}$. Then we set

$$p_{\tau}: \Gamma_{\tau} \setminus V_{\tau} \to \mathbb{C} ,$$

$$\pi(z) \mapsto \varphi(z)^{n}$$

- Let s be a cusp and let $\rho \in SL(2, \mathbb{Z})$ with $\rho(s) = \infty$. Then we have

$$\rho\Gamma_s\rho^{-1}\cdot\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}\}=\{\pm\begin{pmatrix}1&h\\0&1\end{pmatrix}^m\mid m\in\mathbb{Z}\}\text{ for some }h\in\mathbb{N}.$$

We define p_s by

$$p_s: \Gamma_s \setminus V_s \to \mathbb{C},$$

 $\pi(z) \mapsto \exp(2\pi i \varrho(z)/h).$

If we have n > 1 or h > 1 within one of the above maps, the respective point t is a branch point.

The explanations given so far are summarized in the following proposition.

Proposition 4.1.1.

Let Γ be a subgroup of finite index in $SL(2, \mathbb{Z})$. Then $X_{\Gamma} = \Gamma \setminus \mathfrak{H}^*$ is a projective algebraic curve over \mathbb{C} .

Proof.

By the complex structure given above, X_{Γ} is a compact analytic manifold of dimension 1 over \mathbb{C} . By a theorem whose origin may be traced back to Riemann (see [Hart77, App. B, Th. 3.1]), X_{Γ} is a projective algebraic curve over \mathbb{C} .

We conclude from the compactness that X_{Γ} contains only finitely many cusps and elliptic points. For example, $X_{\mathrm{SL}(2,\mathbb{Z})} = \mathrm{SL}(2,\mathbb{Z}) \setminus \mathfrak{H}^*$ has exactly one cusp, represented by ∞ , and one elliptic point of order 2 and 3, respectively, representatives being the complex numbers *i* and $e^{2\pi i/3}$, respectively. If we are given a subgroup Γ of finite index in $\mathrm{SL}(2,\mathbb{Z})$, the curve X_{Γ} is a covering of $X_{\mathrm{SL}(2,\mathbb{Z})}$, and any possible elliptic point on it necessarily has order 2 or 3.

One important topological invariant of any non-singular algebraic curve is its genus. An orientable surface of genus $g \ge 0$ is homeomorphic to the surface of a sphere to which we have attached g handles. The genus $g(X_{\Gamma})$ may be defined by the rank of the first homology group of X_{Γ} with coefficients in \mathbb{Z} . We have the following isomorphisms of abelian groups (see [Shim71, p. 18])

$$H_1(X_{\Gamma}, \mathbb{Z}) \cong H_1(\Gamma, \mathbb{Z}) \cong \mathbb{Z}^{2g(X_{\Gamma})}.$$

For the genus of X_{Γ} we have the following general proposition.

Proposition 4.1.2.

Let Γ be a subgroup of finite index in $SL(2, \mathbb{Z})$. Then the genus of X_{Γ} satisfies

$$g(X_{\Gamma}) = 1 + \frac{n_{\Gamma}}{12} - \frac{s(\Gamma)}{2} - \frac{e_2(\Gamma)}{4} - \frac{e_3(\Gamma)}{3},$$

where

 n_{Γ} is the index $(\text{PSL}(2, \mathbb{Z}) : \overline{\Gamma})$, $s(\Gamma)$ is the number of cusps of X_{Γ} , $e_m(\Gamma)$ is the number of elliptic points of order m on X_{Γ} .

Proof.

See [Shim71, Prop. 1.40]. Proof is performed by applying the Hurwitz Genus Formula to the covering $X_{\Gamma} \to X_{\mathrm{SL}(2,\mathbb{Z})}$.

Moreover, we observe that the number $s(\Gamma)$ of cusps of Γ coincides with the number of double cosets of $\Gamma \setminus \mathrm{SL}(2, \mathbb{Z})/\Gamma_{\infty}$.

The general statements given above are now applied to two important special cases. For $N \in \mathbb{N}$ we consider

$$\Gamma(N) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{SL}(2, \mathbb{Z}) \mid a \equiv d \equiv 1, b \equiv c \equiv 0 \mod N \}, \quad (4.2)$$

$$\Gamma_0(N) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{SL}(2, \mathbb{Z}) \mid c \equiv 0 \mod N \}.$$

$$(4.3)$$

Being the kernel of the reduction map modulo N, $\Gamma(N)$ is a normal subgroup of $SL(2, \mathbb{Z}) = \Gamma(1)$, and is called *principal congruence subgroup* of level N. Any subgroup Γ of $SL(2, \mathbb{Z})$ satisfying $\Gamma(N) \leq \Gamma$ is called *congruence subgroup* of level N. If Γ has the finite index n in $SL(2, \mathbb{Z})$, we have $\Gamma(n) \leq \Gamma$, but in general n is not the smallest possible level of Γ .

 $\Gamma_0(N)$ is a congruence subgroup of level N. By Proposition 4.1.1 the quotient space $X_0(N) = \Gamma_0(N) \setminus \mathfrak{H}^*$ is an algebraic curve over \mathbb{C} , called *modular* curve of level N.

In the sequel, we will examine elliptic modular curves $X_0(N)$, i. e. modular curves $X_0(N)$ of genus 1 for which the investigation is simpler due to the fact that they may be identified with their associated Jacobian varieties. The genus of $X_0(N)$ may be calculated explicitly by means of the formula in Proposition 4.1.2.

Proposition 4.1.3.

Using the notations of Proposition 4.1.2, we have for $\Gamma = \Gamma_0(N)$

$$n_{\Gamma} = N \cdot \prod_{p|N} (1 + \frac{1}{p}),$$

$$e_2(\Gamma) = \begin{cases} 0 & \text{if } 4|N, \\ \prod_{p|N} (1 + (\frac{-1}{p})) & \text{else}, \end{cases}$$

$$e_3(\Gamma) = \begin{cases} 0 & \text{if } 2|N \text{ or } 9|N, \\ \prod_{p|N} (1 + (\frac{-3}{p})) & \text{else}, \end{cases}$$

$$s(\Gamma) = \sum_{d|N} \varphi((d, \frac{N}{d})).$$

Proof. See [Shim71, Prop. 1.43].

Since the expression for the index n_{Γ} dominates all other terms, the genus of $X_0(N)$ tends to ∞ together with N. Especially, there are only finitely many modular curves $X_0(N)$ of any given genus.

If in particular N is a prime number, we have

$$g(X_0(N)) = \begin{cases} \frac{N+1}{12}, & \text{if } N \equiv -1 \mod 12, \\ \lfloor \frac{N-2}{12} \rfloor & \text{else.} \end{cases}$$

The genus of $X_0(N)$ is equal to 1 exactly for the following values of N:

N = 11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49.

For exactly the first 8 values of N, the respective elliptic modular curve $X_0(N)$ does not have complex multiplication. These 8 curves are subject to our later investigation.

4.2 Modular Forms

We now consider the Riemann surface X_{Γ} formed with respect to a congruence subgroup Γ of SL(2, \mathbb{Z}). The meromorphic functions on X_{Γ} correspond bijectively to meromorphic functions $\mathfrak{H} \to \mathbb{C}$ satisfying certain invariance and continuation properties. They form a special case of modular functions which are described below and which are interpreted as meromorphic differential forms on X_{Γ} .

We define for all $k \in \mathbb{Z}$ and all transformations $\alpha = t_A$ corresponding to a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{GL}(2, \mathbb{R})$ with $\det(A) > 0$ the operator $|[\alpha]_k$ on the space of meromorphic functions $f : \mathfrak{H} \to \mathbb{C}$ by

$$(f|[\alpha]_k)(\tau) = \left(\frac{d(\alpha(\tau))}{d\tau}\right)^{k/2} f(\alpha(\tau))$$

= $\frac{(ad - bc)^{k/2}}{(c\tau + d)^k} f\left(\frac{a\tau + b}{c\tau + d}\right).$ (4.4)

The last expression only depends on the transformation α , but not on the representing matrix A.

A function $f : \mathfrak{H} \to \mathbb{C}$ is called *modular function of weight k with respect* to Γ if it satisfies the following conditions:

- 1. f is meromorphic on \mathfrak{H} .
- 2. $f|[\alpha]_k = f$ holds for all $\alpha \in \overline{\Gamma}$.

3. f is meromorphically continuable at every cusp of X_{Γ} .

Another expression for Condition 2 is

$$f(\tau)(d\tau)^{k/2} = f(\alpha(\tau))(d\alpha(\tau))^{k/2}.$$
 (4.5)

Since Γ is a congruence subgroup, Γ contains the element $\binom{1 \ N}{0 \ 1}$ for some $N \in \mathbb{N}$ (for example $N = (\Gamma(1) : \Gamma)$). Then Condition 2 requires of f to have the real period N, and Condition 3 may be stated as follows.

Let s be a cusp of X_{Γ} and $\rho \in SL(2, \mathbb{Z})$ any transformation with $\rho(s) = \infty$. Then $f|[\rho^{-1}]_k$ has a Fourier expansion of the shape

$$f|[\rho^{-1}]_k(\tau) = \sum_{n \ge n_0} c_n q^{n/N} \quad \text{with } q = e^{2\pi i \tau}.$$
 (4.6)

The modular function f is called *modular form*, if it is holomorphic on \mathfrak{H} and at all cusps. In this situation the Fourier expansion (4.6) at any cusp satisfies $n_0 = 0$, i. e. all coefficients of negative index are equal to 0. The value of fat the respective cusp is then given by the coefficient c_0 . The modular form f is called *cusp form*, if its value is equal to 0 at all its cusps, hence if all respective Fourier expansions start at $n_0 = 1$.

We denote by $F_k(\Gamma)$ the complex vector space of modular functions of weight k with respect to Γ , by $M_k(\Gamma)$ the subspace of modular forms, and by $S_k(\Gamma)$ the subspace of cusp forms.

The modular functions of weight 0 form a field which may be interpreted as the field of meromorphic functions on the Riemann surface X_{Γ} . The dimensions of the complex vector spaces $M_k(\Gamma)$ and $S_k(\Gamma)$ are finite, they may be calculated by means of the Theorem of Riemann-Roch (see [Shim71, Thm. 2.23, 2.24, 2.25]).

If $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ is an element of the congruence subgroup Γ , there is no non-zero modular function of odd weight with respect to Γ . This observation simplifies our considerations for all groups $\Gamma_0(N)$ since in these cases we only encounter integral exponents in (4.4) and (4.5).

The following functions are examples of modular functions with respect to $SL(2, \mathbb{Z})$ whose Fourier expansions at the cusp ∞ are given in terms of the parameter $q = e^{2\pi i \tau}$.

- The Eisenstein series G_{2k} is a modular form of weight 2k,

$$G_{2k}(\tau) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m\tau+n)^{2k}}$$
$$= 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} d_{2k-1}(n)q^n,$$

with $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ and $d_r(n) = \sum_{d|n} d^r$. In the following examples we use the classical notations

$$g_2(\tau) = 60 \ G_4(\tau)$$
 and $g_3(\tau) = 140 \ G_6(\tau)$.

– The Δ -function is a cusp form of weight 12,

$$\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$$
$$= (2\pi)^{12}q \prod_{n=1}^{\infty} (1-q^n)^{24}$$

- The *j*-function is a modular function of weight 0,

$$j(\tau) = \frac{1728g_2(\tau)^3}{\Delta(\tau)}$$
$$= \frac{1}{q} + 744 + \sum_{n \ge 1} c_n q^n \quad \text{with } c_n \in \mathbb{Z}.$$

We are able to express the structure of the spaces of modular forms with respect to $SL(2, \mathbb{Z})$ by means of the functions we have just described.

Proposition 4.2.1.

(a) For $k \geq 2$ we have an isomorphism of \mathbb{C} -vector spaces

$$M_{2k}(\mathrm{SL}(2,\mathbb{Z})) \cong S_{2k}(\mathrm{SL}(2,\mathbb{Z})) \oplus \mathbb{C} G_{2k}$$

- (b) For all $k \in \mathbb{Z}$, $m_{\Delta} : M_{2k-12}(\mathrm{SL}(2,\mathbb{Z})) \to S_{2k}(\mathrm{SL}(2,\mathbb{Z}))$, $f \mapsto f \cdot \Delta$, is an isomorphism of \mathbb{C} -vector spaces.
- (c) The \mathbb{C} -dimension of $M_{2k}(\mathrm{SL}(2,\mathbb{Z}))$ is given by

$$\dim_{\mathbb{C}} M_{2k}(\mathrm{SL}(2, \mathbb{Z})) = \begin{cases} 0 & \text{if } k < 0, \\ [k/6] & \text{if } k \ge 0, k \equiv 1 \mod 6, \\ [k/6] + 1 & \text{if } k \ge 0, k \not\equiv 1 \mod 6. \end{cases}$$

Proof. See [Silv94, I. 3.10].

The field of meromorphic functions on $X_0(N)$ may be described in terms of the *j*-function. Using the notation $j_N(\tau) = j(N\tau)$, we have the following proposition.

Proposition 4.2.2. We have $F_0(\Gamma_0(N)) = \mathbb{C}(j, j_N)$.

Proof. See [Shim71, Prop. 2.10].

Proposition 4.2.2 enables us to conclude that the modular curve $X_0(N)$ which is originally defined over \mathbb{C} arises from an algebraic curve over \mathbb{Q} .

Corollary 4.2.1.

The modular curve $X_0(N)$ is defined over \mathbb{Q} . More precisely, there is a nonsingular projective curve X_N over \mathbb{Q} such that $X_0(N)$ may be identified with the set $X_N(\mathbb{C})$ obtained by extending the range of coordinates from \mathbb{Q} to \mathbb{C} .

Proof.

The function field of $X_0(N)$ is equal to $\mathbb{C}(j, j_N)$ which is a field extension of \mathbb{C} of transcendence degree 1. j_N is algebraic over $\mathbb{C}(j)$, thus there is a polynomial $\Phi_N(x, y) \in \mathbb{C}[x, y]$ with $\Phi_N(j, j_N) = 0$. Since the *j*-function has a Fourier expansion with integral coefficients, we infer $\Phi_N(x, y) \in \mathbb{Q}[x, y]$. $\Phi_N(x, y) = 0$ defines therefore an algebraic curve over \mathbb{Q} which is singular in general. However, the procedure of desingularization ensures the existence of a non-singular projective algebraic curve X_N over \mathbb{Q} having the function field $\mathbb{Q}(j, j_N)$, so that $X_N(\mathbb{C})$ becomes a Riemann surface isomorphic to $X_0(N)$. See also the generalization in [Shim71, 6.7, p. 156f].

This result enables us to apply reduction modulo primes p to $X_0(N)$.

4.3 Hecke Operators

Hecke operators appear in several different connections. We have therefore to postulate a sufficiently abstract definition in order to allow a unified treatment. The most general approach can be found in [Shim71, chap. 3] which is here applied to the special case of subgroups Γ of finite index in SL(2, \mathbb{Z}) and the multiplicative semigroup

$$\Delta = \{ \alpha \in M(2, \mathbb{Z}) \mid \det \alpha > 0 \}.$$

Then the *Hecke ring* $R(\Gamma, \Delta)$ is the free **Z**-module generated by the double cosets in $\Gamma \setminus \Delta/\Gamma$,

$$R(\Gamma, \Delta) = \{ \sum_{i} c_{i} \cdot \Gamma \alpha_{i} \Gamma \mid \alpha_{i} \in \Delta, c_{i} \in \mathbb{Z} \}.$$

For $n \in \mathbb{N}$, the Hecke operator T_n is the element of $R(\Gamma, \Delta)$ defined by

$$T_n = \sum_{\det \alpha = n} \Gamma \alpha \Gamma \quad , \tag{4.7}$$

where the sum runs over all double cosets in $\Gamma \Delta \Gamma$ which may be written in the form $\Gamma \alpha \Gamma$ with det $\alpha = n$.

The operation of the Hecke ring on the space $F_k(\Gamma)$ of modular functions of level k with respect to Γ is initially defined on the basis elements $\Gamma \alpha \Gamma$. Let α_i run through a system of representatives of the right cosets contained in $\Gamma \alpha \Gamma$,

$$\Gamma \alpha \Gamma = \bigcup_{j} \Gamma \alpha_{j}.$$

Then we set

$$f|[\Gamma \alpha \Gamma]_k = (\det \alpha)^{\frac{k}{2}-1} \sum_j f|[\alpha_j]_k.$$

This operation is extended by linearity to all of $R(\Gamma, \Delta)$.

In particular, the Hecke operator T_n induces an operator $T_n^{(k)}$ on $F_k(\Gamma)$ by

$$T_n^{(k)}(f) = n^{\frac{k}{2}-1} \sum_{\alpha \in \mathcal{R}_n} f|[\alpha]_k ,$$

where \mathcal{R}_n is a system of representatives of those right cosets which are contained in the union of the double cosets appearing in (4.7).

For the congruence subgroups $\Gamma_0(N)$ of $SL(2, \mathbb{Z})$, \mathcal{R}_n is given by

$$\mathcal{R}_n = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix} \right) \in M(2, \mathbb{Z}) \mid a \, d = n \, , \, a > 0 \, , \, (a, N) = 1 \, , \, 0 \le b < d \right\} \, ,$$

and we are able to explicitly calculate the Hecke operator $T_n^{(k)}$ on $F_k(\Gamma_0(N))$ as

$$T_{n}^{(k)}(f)(\tau) = n^{k-1} \sum_{\substack{d|n\\ (\frac{n}{d}, N)=1}} d^{-k} \sum_{b=0}^{d-1} f\left(\frac{n\tau + bd}{d^{2}}\right).$$
(4.8)

When defining the Hecke operators in the special case of the congruence subgroups $\Gamma_0(N)$, we may instead use another, more geometric approach in terms of lattices in the complex plane. We have to exclude the cusps and consider $Y_0(N) = \Gamma_0(N) \setminus \mathfrak{H}$ instead of $X_0(N)$.

 $Y_0(1)$ is interpreted as moduli space, i. e. as a parameter space for the isomorphy classes of elliptic curves over C. By the Uniformization Theorem (see [Silv86, VI. 5.1]) any elliptic curve over \mathbb{C} is isomorphic to a quotient \mathbb{C}/Λ with a lattice Λ in \mathbb{C} , and two elliptic curves $E \cong \mathbb{C}/\Lambda$, $E' \cong \mathbb{C}/\Lambda'$ are isomorphic over \mathbb{C} if and only if there is an $a \in \mathbb{C}^*$ satisfying $a\Lambda = \Lambda'$, i. e. if and only if the lattices Λ and Λ' are homothetic.

In each homothety class of lattices in \mathbbm{C} we find a representative of the form

$$\Lambda_{\tau} = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau \text{ with } \operatorname{Im}(\tau) > 0, \qquad (4.9)$$

and we have $\mathbb{C}/\Lambda_{\tau} \cong \mathbb{C}/\Lambda_{\tau'}$ if and only if $\tau' = \frac{a\tau+b}{c\tau+d}$ with $\binom{a\ b}{c\ d} \in \mathrm{SL}(2,\mathbb{Z})$. Thus $X_0(1)$ parametrizes the isomorphy classes of elliptic curves over \mathbb{C} by the bijection $\tau \mapsto \mathbb{C}/\Lambda_{\tau}$.

In general, we interpret $Y_0(N)$ as a moduli space for pairs (Λ, C) , where Λ is a lattice in \mathbb{C} and C is an additive cyclic subgroup of \mathbb{C}/Λ of the order N. The notion of homothety may be transferred to these pairs. In each homothety class we find at least one representative of the form (Λ_{τ}, C_N) with Λ_{τ} as in (4.9) and with $C_N = \frac{1}{N} + \Lambda_{\tau}$, and two pairs (Λ_{τ}, C_N) , $(\Lambda_{\tau'}, C_N)$ are homothetic if and only if we have $\tau' = \frac{a\tau+b}{c\tau+d}$ with $\binom{a\ b}{c\ d} \in \Gamma_0(N)$. Let $R_N = \mathbb{Z}[(\Lambda, C) \mid \Lambda$ lattice in $\mathbb{C}, C \leq \mathbb{C}/\Lambda$ cyclic of the order N] be

Let $R_N = \mathbb{Z}[(\Lambda, C) \mid \Lambda \text{ lattice in } \mathbb{C}, C \leq \mathbb{C}/\Lambda \text{ cyclic of the order } N]$ be the free abelian group generated by the pairs (Λ, C) . We define the Hecke operator T_n on the basis elements of R_N by

$$T_n(\Lambda, C) = \sum_{\substack{[\Lambda:\Lambda']=n\\|nC|=N}} (\Lambda', nC) , \qquad (4.10)$$

where the sum runs through all lattices Λ' which are sublattices of Λ of index n so that the cyclic subgroup nC of \mathbb{C}/Λ' still has the order N. The sum is finite because the lattice $n\Lambda$ is contained in all lattices Λ' so that Λ' is already uniquely determined by the finitely many elements of $\Lambda'/n\Lambda$.

The modular functions f in $F_k(\Gamma_0(N))$ may be interpreted as functions φ_f on lattices Λ , or on pairs (Λ, C) as above, respectively, which are constant on homothety classes. They are defined by $\varphi_f((\Lambda_\tau, C)) = f(\tau)$, the invariance and homogenity properties of $F_k(\Gamma_0(N))$ ensuring the well-definition of φ_f . The effect of the Hecke operator is then given by

$$T_n^{(k)}(\varphi_f)((\Lambda_{\tau}, C)) = n^{k-1} \sum_{[\Lambda_{\tau}:\Lambda']=n \atop |nC|=N} \varphi_f((\Lambda', nC)) .$$

After performing suitable transformations, we obtain a representation of the form (4.8) for $T_n^{(k)}(f)$. Thus $T_n^{(k)}(f)$ essentially calculates the average of the values of the function f at the points which correspond to sublattices of index n conserving the order of a certain subgroup. The set \mathcal{R}_n turns out to be a system of representatives of transformations which perform the transition to these sublattices.

In the sequel, only the Hecke operators $T_n^{(k)}$ on the modular functions in $F_k(\Gamma_0(N))$ are of particular importance. We restrict therefore our attention to this special case.

Proposition 4.3.1.

Let the Fourier expansion of the function f from $F_k(\Gamma_0(N))$ have the shape $f(\tau) = \sum_{m \ge m_0} c_m q^m$ at ∞ . Then $T_n^{(k)}(f)$ has the Fourier expansion (with $m_1 \ge \min\{0, nm_0\})$

$$T_n^{(k)}(f)(\tau) = \sum_{m \ge m_1} d_m q^m \quad with \quad d_m = \sum_{a \mid (m,n) \atop (a,N) = 1} a^{k-1} c_{\frac{mn}{a^2}}$$

Proof.

This result is achieved by direct calculation (cf. [Silv94, I. Prop. 10.3]). $\hfill\square$

In particular, we find $d_1 = c_n$ and $d_0 = c_0 \sum_a a^{k-1}$, which leads us to the following corollary.

Corollary 4.3.1.

The Hecke operators $T_n^{(k)}$ map the spaces of modular forms and cusp forms to themselves, i. e. they induce operators $T_n^{(k)} : M_k(\Gamma_0(N)) \to M_k(\Gamma_0(N))$ and $T_n^{(k)} : S_k(\Gamma_0(N)) \to S_k(\Gamma_0(N)).$

The composition of Hecke operators is described by the following proposition.

Proposition 4.3.2.

(a) The Hecke operators are multiplicative, i. e. they satisfy

$$T_m^{(k)}T_n^{(k)} = T_{mn}^{(k)} \quad for \quad (m,n) = 1.$$

(b) For prime numbers p and all $r \ge 1$ we have the formulas

$$T_{p^{r+1}}^{(k)} = T_p^{(k)} T_{p^r}^{(k)} - p^{k-1} T_{p^{r-1}}^{(k)}, \quad \text{if } p \text{ does not divide } N, \\
 T_{p^r}^{(k)} = (T_p^{(k)})^r, \quad \text{if } p \text{ divides } N.$$
(4.11)

Proof.

See [Knap92, Thm. 9.17].

The following corollary summarizes Proposition 4.3.2 into one formula and stresses an essential consequence of it.

Corollary 4.3.2.

(a) The Hecke operators $T_n^{(k)}$ satisfy the composition rule

$$T_m^{(k)} T_n^{(k)} \; = \; \sum_{a \mid (m,n) \atop (a,N) = 1} a^{k-1} \, T_{a^2}^{(k)} \; .$$

(b) The Hecke operators are mutually commutative, i. e. we have

$$T_m^{(k)}T_n^{(k)} = T_n^{(k)}T_m^{(k)} \quad for \quad m, n \in \mathbb{N}.$$

Thus the effect of all Hecke operators $T_n^{(k)}$ is unambiguously determined once we know the operators $T_p^{(k)}$ that have prime number index p.

We gain further insight into the structure of the operation of $T_n^{(k)}$ by examining eigenfunctions and eigenvalues. A simple but central result can be concluded directly from Proposition 4.3.1.

Corollary 4.3.3.

- (a) Let $f \in F_k(\Gamma_0(N))$ be an eigenfunction of the operator $T_n^{(k)}$ having the eigenvalue $\lambda(n) \in \mathbb{C}$. If $f(\tau) = \sum_{n \ge n_0} c_n q^n$ with $q = e^{2\pi i \tau}$ is the Fourier expansion of f, we have $c_n = \lambda(n) c_1$.
- (b) If $f \in S_k(\Gamma_0(N))$ is an eigenfunction for all operators $T_n^{(k)}$ with $n \in \mathbb{N}$, f is uniquely determined up to a constant factor.

Hence, if the cusp form $f(\tau) = \sum_{n\geq 1} c_n q^n$ is a simultaneous eigenform of all Hecke operators, we have $c_1 \neq 0$ because f is not identically 0. If we normalize f by letting $c_1 = 1$, the Fourier coefficient c_n of f coincides with the eigenvalue $\lambda(n)$ of f with respect to the Hecke operator $T_n^{(k)}$.

We may define a hermitian product called the *Petersson product* on the complex vector space $S_k(\Gamma_0(N))$ of cusps forms by

$$\langle f,g \rangle_k = \int_{X_0(N)} f(x+iy) \overline{g(x+iy)} y^{k-2} dx dy .$$

The integral extends over a fundamental domain of $X_0(N)$, i. e. over the closure of a simply connected system of representatives of $\Gamma_0(N) \setminus \mathfrak{H}^*$ in \mathfrak{H}^* . The convergence of the integral is assured by the fact that both argument functions are cusp forms.

Proposition 4.3.3.

For all $n \in \mathbb{N}$ with (n, N) = 1 the Hecke operators $T_n^{(k)}$ on $S_k(\Gamma_0(N))$ are self adjoint with respect to the Petersson product, *i. e.* we have the formula

$$\langle T_n^{(k)}(f), g \rangle_k = \langle f, T_n^{(k)}(g) \rangle_k$$
.

Proof.

See [Knap92, Thm. 9.18].

By a result of linear algebra, each family of mutually commuting, self adjoint operators on a finite dimensional vector space has an orthogonal basis whose elements are simultaneous eigenvectors of all operators (see for example [Gant86, 9.15 Satz 11]).

In the situation dealt with here, we have an orthogonal sum decomposition $S_k(\Gamma_0(N)) = \bigoplus_i V_i$, the elements of V_i being simultaneous eigenfunctions of all Hecke operators $T_n^{(k)}$ for $n \in \mathbb{N}$ with (n, N) = 1. All elements of V_i have the same eigenvalue $\lambda_i(n)$ with respect to the Hecke operator $T_n^{(k)}$. The system of eigenvalues $\{\lambda_i(n) \mid n \in \mathbb{N}, (n, N) = 1\}$ is therefore an invariant of V_i .

The Hecke operators $T_p^{(k)}$ with p|N are generally not self adjoint, not even diagonalizable. But since all Hecke operators are mutually commutative, they respect the above decomposition, i. e. we have $T_p^{(k)}(V_i) \subseteq V_i$ for all i, and in each space V_i we find at least one element which is a common eigenfunction of all Hecke operators $T_n^{(k)}$ with $n \in \mathbb{N}$.

Corollary 4.3.4.

Let $f \in S_k(\Gamma_0(N))$ be a normalized cusp form which is a simultaneous eigenform of all Hecke operators $T_n^{(k)}$ with $n \in \mathbb{N}$. Then the coefficients c_n of the Fourier expansion of f at ∞ are multiplicative and satisfy the following formulas similar to the $T_n^{(k)}$ in (4.11) for all prime numbers p and all $r \in \mathbb{N}$

$$c_{p^{r+1}} = c_{p^r}c_p - p^{k-1}c_{p^{r-1}}, \quad \text{if } p \text{ does not divide } N, \\ c_{p^r} = c_p^r, \quad \text{if } p \text{ divides } N.$$

If $f \in S_k(\Gamma_0(N))$ is a cusp form having the Fourier expansion

$$f(\tau) = \sum_{n \ge 1} c_n q^n , \quad q = e^{2\pi i \tau} .$$

we define the L-series of f by

$$L_f(s) = \sum_{n \ge 1} c_n n^{-s}.$$
 (4.12)

The series in (4.12) is convergent for all $s \in \mathbb{C}$ satisfying $\operatorname{Re}(s) > \frac{k}{2} + 1$ (cf. [Silv94, I. Thm. 11.2] or [Knap92, Lemma 9.6]).

The multiplicativity and the recursion formula of the Fourier coefficients c_n in Corollary 4.3.4 are formally equivalent to the following product identity.

Corollary 4.3.5.

Let $f \in S_k(\Gamma_0(N))$ be a normalized cusp form whose Fourier expansion at ∞ is given by $f(\tau) = \sum_{n \ge 1} c_n q^n$, $q = e^{2\pi i \tau}$, and which is a simultaneous eigenform of all Hecke operators $T_n^{(k)}$ with $n \in \mathbb{N}$. Then the L-series of f satisfies

$$L_f(s) = \prod_{p|N} \frac{1}{1 - c_p p^{-s}} \prod_{p \not\mid N} \frac{1}{1 - c_p p^{-s} + p^{2k - 1 - 2s}} \, .$$

The structure of the spaces V_i under the operation of the $T_p^{(k)}$ with p|N is uncovered in [AtLe70]. The problems concerning the diagonalizability in $S_k(\Gamma_0(N))$ are caused by the so-called old forms which result from elements of a space $S_k(\Gamma_0(M))$ for some proper divisor M of N.

4.4 The Eichler-Shimura Formula

The central result of this section is the Eichler-Shimura Formula which provides an intimate connection between function theory and arithmetic of the modular curves $X_0(N)$. As a preparation, we interpret Hecke operators as algebraic correspondences, and we explain the principle of reduction modulo p.

Let C_1, C_2 be two projective non-singular curves. The group of (proper) algebraic correspondences between C_1 and C_2 is defined as

$$\mathcal{A}(C_1, C_2) = \mathbb{Z} \left[\begin{array}{c} D \mid D \text{ 1-dimensional (proper) subvariety of } C_1 \times C_2 \end{array} \right]$$
$$= \left\{ \sum_i n_i D_i \mid n_i \in \mathbb{Z}, \ D_i \subset C_1 \times C_2, \ \dim(D_i) = 1 \end{array} \right\}.$$

Thus the basis elements of the algebraic correspondences from C_1 to C_2 are the non-singular curves contained in $C_1 \times C_2$, curves of the form $C_1 \times \{c\}$ and $\{c\} \times C_2$ being excluded. In $\mathcal{A}(C_1, C_2)$, they are assigned to certain multiplicities of which only finitely many are different from 0.

The basis elements of algebraic correspondences may be understood as relations which generalize the notion of a function. By linear extension, we are able to transfer operations on relations to operations on correspondences. Two important special cases are as follows:

- If $K \subset C_1 \times C_2$ and $L \subset C_2 \times C_3$ are non-singular curves, the *composition* $L \circ K$ is defined as a subset of $C_1 \times C_3$ in the usual way,

$$L \circ K = \{ (u, w) \mid \text{ there is a } v \in C_2 \text{ with } (u, v) \in K \text{ and } (v, w) \in L \}.$$

This is a non-singular curve contained in $C_1 \times C_3$.

- If $K \subset C_1 \times C_2$ is as above then we get the *transposed* (or *dual*) correspondence K^t with respect to K by interchanging the components,

$$K^{t} = \{ (u, v) \mid (v, u) \in K \}.$$

If C is a non-singular curve, the algebraic correspondences from C to C form a ring $\mathcal{A}(C)$ with respect to composition and addition. Transposition provides an involution of $\mathcal{A}(C)$.

Algebraic correspondences offer an elegant way to describe certain wellshaped assignments from elements of C_1 to elements of C_2 . For example, if $f: C_1 \to C_2$ is a rational mapping, the graph of f,

$$\Gamma_f = \{ (x, f(x)) \mid x \in C_1 \},\$$

is an algebraic correspondence lying in $\mathcal{A}(C_1, C_2)$.

We will interpret the Hecke operators T_n mentioned in Section 4.3 as correspondences of the modular curve $X_0(N)$. Because of the intended multiplicativity and because of the recursion formula (cf. (4.11)) we restrict ourselves to Hecke operators T_p having prime number index p, where for simplicity reasons we additionally exclude the finitely many prime divisors of N. Thus, in the following let p always denote a prime number which does not divide N. If for such p we let

$$T_p = \{ (\overline{\tau}, \overline{p\tau}) \mid z \in \mathfrak{H}^* \}, \tag{4.13}$$

where $\overline{\tau}$ denotes the image of τ under the canonical projection $\mathfrak{H}^* \to X_0(N)$, T_p proves to be an algebraic correspondence on $X_0(N) \times X_0(N)$, even an algebraic curve defined over \mathbb{Q} [Shim71, 7.3, Prop. 7.2 and p. 176] which is isomorphic to $X_0(pN)$ [Shim71, 3.4 p. 76f].

More informally, each pair of values (t, t') in the correspondence T_p comes with a pair $(j(\mathbb{C}/\Lambda_{\tau}), j(\mathbb{C}/\Lambda_{\tau'}))$ of *j*-invariants, where Λ_{τ} is a lattice in \mathbb{C} and $\Lambda_{\tau'}$ is a sublattice of index p in Λ_{τ} . When we settle T_p in this way and keep in mind our assumption p/N, we observe that this definition is equivalent to (4.7) and (4.10). To any fixed value of t, T_p contains exactly p+1 pairs (t, t'), and a similar statement holds for fixed t'.

In order to establish a connection to the L-series of $X_0(N)$, we have to apply reduction modulo p to the curve $X_0(N)$ and to the correspondences given above. Our aim is to find for all geometric objects appearing in the context of the curve $X_0(N)$ defined over $\overline{\mathbb{Q}}$ their respective counterpart over $\overline{\mathbb{F}}_p$. Some functorial properties of the principle of reduction modulo p are summarized in [Shim58, 9.] and [Shim71, 7.4]. In particular, correspondences are mapped to correspondences and non-singular algebraic curves of genus g are mapped to algebraic curves which also have genus g if they are non-singular. The reduction of an elliptic curve is obtained by interpreting a defining equation over \mathbb{Q} of the form (3.1) as an equation over \mathbb{F}_p .

Since p is no divisor of N, $X_0(N)$ has good reduction at p, i. e. we are able to find an equation of the form (3.1) having integral coefficients and a discriminant which is not divisible by p. The reduction of this equation modulo p defines a non-singular curve $\tilde{X}_0(N)$ over \mathbb{F}_p .

The graph of the restriction of the geometric Frobenius automorphism $\pi_p: \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p, x \mapsto x^p$, to $\tilde{X}_0(N)$ forms the algebraic correspondence

$$\Pi_p = \{ (x, x^p) \mid x \in X_0(N) \}.$$

We can reduce the Hecke operator T_p modulo p to give a correspondence \tilde{T}_p on $\tilde{X}_0(N)$, if we apply the construction described above in terms of j-invariants over $\overline{\mathbb{F}}_p$ (see [SwBi75, p. 14f]).

The next theorem states the main result of this section, by which we are able to interpret the reduction of the Hecke operator T_p modulo p on $\tilde{X}_0(N)$ as the trace of the Frobenius automorphism.

Theorem 4.4.1. (Eichler-Shimura Formula)

Let p be a prime number which does not divide N. Then the reduction $\tilde{T_p}$ of the p-th Hecke operator modulo p satisfies the identity

$$\tilde{T}_p = \Pi_p + \Pi_p^t .$$

Theorem 4.4.1 was at first proved by M. Eichler and later largely generalized by G. Shimura (see [Eich54], [Shim58, 11.] and [Shim71, Cor. 7.10]).

In order to use an additive structure in the proof of Theorem 4.4.1, we have to work with the Jacobian variety \tilde{J}_N of $\tilde{X}_0(N)$. Similar to Section 3.5, we construct on \tilde{J}_N for all prime numbers ℓ which do not divide pN the ℓ -adic Tate-module $T_\ell(\tilde{J}_N)$ as the projective limit of the ℓ -power torsion points with respect to the multiplication $[\ell]$,

$$T_{\ell}(\tilde{J}_N) = \lim_{\longleftarrow} \ker([\ell^n] : \tilde{J}_N \to \tilde{J}_N) .$$

 $T_{\ell}(\tilde{J}_N)$ proves to be a free \mathbb{Z}_{ℓ} -module of rank $2g_N$ if g_N denotes the genus of $X_0(N)$. As in Section 3.5, we then obtain the $2g_N$ -dimensional ℓ -adic representation

$$r_{\ell} : \operatorname{End}(\tilde{J}_N) \to \operatorname{End} T_{\ell}(\tilde{J}_N)$$

by assigning to each endomorphism of \tilde{J}_N the induced operation on the ℓ^n -torsion points.

We define the *p*-adic factor of the L-series of $X_0(N)$ by

$$L_p(T) = \det(\mathbf{1} - r_\ell(\pi_p) T) , \qquad (4.14)$$

if π_p denotes the Frobenius endomorphism of \tilde{J}_N and ℓ is a prime number which does not divide pN. From the Eichler-Shimura Formula we then get the following corollary.

Corollary 4.4.1.

If p is a prime number which does not divide N and $T_p^{(2)}$ is the Hecke operator on the g_N -dimensional space $S_2(\Gamma_0(N))$, we have the relation

$$L_p(T) = \det(\mathbf{1} - T_p^{(2)}T + pT^2)$$
$$= \prod_{i=1}^{g_N} (1 - c_{p,i}T + pT^2),$$

if $c_{p,i}$ runs through the g_N eigenvalues of $T_p^{(2)}$.

Proof.

See [Shim71, Thm. 7.11] or [SwBi75]).

If $X_0(N)$ is an elliptic modular curve, that is, if $X_0(N)$ has genus $g_N = 1$, all prime numbers p not dividing N satisfy

$$\det(\mathbf{1} - r_{\ell}(\pi_p)T) = 1 - a_p T + p T^2,$$

where $a_p = p + 1 - \# \tilde{X}_0(N)(\mathbb{F}_p)$ depends on the number of \mathbb{F}_p -rational points of $\tilde{X}_0(N)$ (cf. (3.11)).

By Corollary 4.4.1 we have the equality $c_p = a_p$ for these p, if c_p denotes the eigenvalue of the Hecke operator $T_p^{(2)}$. Hence, in the case of elliptic modular curves $X_0(N)$, we may interpret the trace of the ℓ -adic representation of the Frobenius automorphism π_p both as an arithmetic quantity (the number of points of $\tilde{X}_0(N)$ over \mathbb{F}_p) and as a function theoretic quantity (the eigenvalue of the p-th Hecke operator).

We may state these observations in terms of L-series if we neglect the Euler factors belonging to the prime divisors p of N. However, in order to formulate results like a functional equation of L-series we are forced to give an appropriate definition of the Euler factors belonging to the prime divisors of N as well. The shape of these factors is predicted by the statement of Corollary 4.3.5. Using (3.16) we infer:

Corollary 4.4.2.

Let $E = X_0(N)$ be an elliptic modular curve and f the unique normalized cusp form in $S_2(\Gamma_0(N))$ which is an eigenfunction of all Hecke operators $T_n^{(2)}$. If we possibly disregard finitely many Euler factors, we have the identity

$$L_{E/\mathbb{Q}}(s) = L_f(s) .$$

In some special cases we are able to express the unique normalized cusp form of weight 2 by the η -function

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1-q^n) \quad , \ q = e^{2\pi i \tau}.$$

The resulting expressions are summarized in Table 4.1. Criteria for the representability are given in [Ligo75, 3.1]. In these cases, the L-series coefficients are in interrelation with the coefficients of an infinite product.

However, there are only finitely many values of N for which $X_0(N)$ is an elliptic modular curve. If $X_0(N)$ is a general modular curve, to each cusp form f in $S_2(\Gamma_0(N))$ which is a common eigenfunction of all Hecke operators there is then an elliptic curve E_f defined over \mathbb{Q} having the conductor N and there is a covering $X_0(N) \to E_f$ such that we have

$$L_{E_f/\mathbb{Q}}(s) = L_f(s).$$

The L-series of f appears therefore as the L-series of an elliptic curve which is a quotient of $X_0(N)$.

N	Normalized Cusp Form	Product Expression
11	$\eta(\tau)^2 \eta(11\tau)^2$	$q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2$
14	$\eta(\tau)\eta(2\tau)\eta(7\tau)\eta(14\tau)$	$q \prod_{n=1}^{\infty} (1-q^n)(1-q^{2n})(1-q^{7n})(1-q^{14n})$
15	$\eta(\tau)\eta(3\tau)\eta(5\tau)\eta(15\tau)$	$q \prod_{n=1}^{\infty} (1-q^n)(1-q^{3n})(1-q^{5n})(1-q^{15n})$
20	$\eta(2\tau)^2\eta(10\tau)^2$	$q \prod_{n=1}^{\infty} (1-q^{2n})^2 (1-q^{10n})^2$
24	$\eta(2\tau)\eta(4\tau)\eta(6\tau)\eta(12\tau)$	$q \prod_{n=1}^{\infty} (1-q^{2n})(1-q^{4n})(1-q^{6n})(1-q^{12n})$

Table 4.1. η -Products of Normalized Weight 2 Cusp Forms on $X_0(N)$

5 Torsion Point Fields

In this chapter we describe Galois extensions of number fields which are obtained by adjoining the coordinates of torsion points of a given order n on an elliptic curve. We formulate conditions ruling the decomposition in these extensions over a number field.

The groups GL(2, n) which may appear as Galois groups of these extensions are examined in Section 5.1. By the Main Theorem of Galois theory, we can uniquely assign a certain subfield of the *n*-torsion point extension to any subgroup of GL(2, n). The most important of these intermediate fields are listed in Section 5.2 and described in greater detail.

Section 5.3 mentions certain defining polynomials of some important subextensions. The special cases of *n*-torsion points with n = 2, 3, 4 are treated in Section 5.4 and Section 5.5. The final section summarizes our results and gives criteria for the decomposition law in p^m -torsion point fields.

5.1 The Groups GL(2,n)

When examining a Galois extension of number fields K/k, it is recommended to determine at first the properties of the Galois group Gal(K/k). Quite often, the Galois group is easier to handle, and by the Main Theorem of Galois theory, any subfield of the extension K/k corresponds bijectively to a subgroup of Gal(K/k). Normal subgroups of Gal(K/k) earn special attention, since they correspond to Galois subfields.

In the case of the *n*-torsion point extensions defined in Section 3.4 the occurring Galois groups are subgroups of GL(2, n), and without any further knowledge we have to assume that any such subgroup may appear as the Galois group of a given *n*-torsion point extension.

As an abstract group, $\operatorname{GL}(2, n)$ describes exactly the automorphisms of the additive group $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, hence

$$\operatorname{GL}(2,n) \cong \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}).$$
 (5.1)

The assignment of the group automorphisms to the respective matrices includes the choice of generators $\{g_1, g_2\}$ of $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Some of the first interesting normal subgroups of GL(2, n) are its center Z(GL(2, n)) and the kernel SL(2, n) of the determinant map.

C. Adelmann: LNM 1761, pp. 59–86, 2001.

 $[\]bigodot$ Springer-Verlag Berlin Heidelberg 2001

Proposition 5.1.1.

(a) The center of GL(2, n) is given by

$$Z(\operatorname{GL}(2,n)) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in (\mathbb{Z}/n\mathbb{Z})^* \right\} \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

(b) The subgroup $G_n \leq \operatorname{GL}(2,n)$ given by $G_n = \{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/n\mathbb{Z})^* \}$ satisfies

$$\operatorname{GL}(2,n) \cong \operatorname{SL}(2,n) \rtimes G_n.$$

(c) We have the following exact sequences of groups

$$1 \to (\mathbb{Z}/n\mathbb{Z})^* \to \operatorname{GL}(2,n) \to \operatorname{PGL}(2,n) \to 1 ,$$

$$1 \to \operatorname{SL}(2,n) \to \operatorname{GL}(2,n) \to (\mathbb{Z}/n\mathbb{Z})^* \to 1 ,$$

the first one given by the projection to $\operatorname{PGL}(2,n) = \operatorname{GL}(2,n)/Z(\operatorname{GL}(2,n))$ and the second one by the map det : $\operatorname{GL}(2,n) \to (\mathbb{Z}/n\mathbb{Z})^*$. The second sequence splits.

Proof.

- (a) Isomorphy on the right hand side is obvious. Likewise it is obvious that the diagonal matrices ^{a 0}_{0 a} for a ∈ (Z/nZ)* are elements of the center. If ^{a b}_{c d}) ∈ Z(GL(2, n)) is an element of the center, it commutes with the matrices ^{1 1}_{0 1}, (^{1 0}_{1 1}) ∈ GL(2, n). We conclude from the resulting identities that we must have ^{a b}_{c d}) ≡ ^{a 0}_{0 a} mod n.
- (b) The assertion can be deduced from SL(2,n) $G_n = GL(2,n)$ and $SL(2,n) \cap G_n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- (c) The first sequence results from (a). In the second one the determinant map is surjective since we have $\det(G_n) = (\mathbb{Z}/n\mathbb{Z})^*$. The second sequence splits by (b).

We now point out the important fact that the decomposition of n into a product of powers of prime numbers gives rise to a decomposition of GL(2, n) into direct factors.

Proposition 5.1.2.

Let $n = p_1^{m_1} \cdot \ldots \cdot p_r^{m_r}$ be the canonical prime factor decomposition of n. Then we have $\operatorname{GL}(2,n) \cong \operatorname{GL}(2,p_1^{m_1}) \times \cdots \times \operatorname{GL}(2,p_r^{m_r})$.

Proof.

The proof is performed by applying the Chinese Remainder Theorem to the matrix entries. The reduction map is compatible with matrix multiplication since it is compatible with the arithmetic operations + and \cdot .

By applying the last proposition we can determine the size of GL(2, n).

Proposition 5.1.3.

The number of elements of GL(2,n) is $|GL(2,n)| = n^4 \prod_{n|n} (1 - \frac{1}{p})(1 - \frac{1}{p^2}).$

Proof.

Let the function $f: \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = |\operatorname{GL}(2, n)|$.

For prime numbers p we have $f(p) = (p^2 - 1)(p^2 - p)$, because this is the number of ordered pairs of linear independent vectors of a 2-dimensional vector space over the finite field \mathbb{F}_p .

For prime powers p^m , $m \in \mathbb{N}$, we have $f(p^m) = p^{4(m-1)}f(p)$, since a matrix $\binom{a \ b}{c \ d}$ having entries in $\mathbb{Z}/p^m\mathbb{Z}$ belongs to $\operatorname{GL}(2, p^m)$ if and only if its reduction modulo p is an element of GL(2, p), and the kernel of the reduction map $\mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ contains exactly p^{m-1} elements.

By Proposition 5.1.2, f(n) is multiplicative in the sense of a number theoretic function, hence f(n) has the asserted form.

In the sequel we will restrict ourselves to the groups $GL(2, p^m)$ for prime powers p^m . The knowledge obtained by examining this special case can be combined into statements on general n with the aid of Proposition 5.1.2.

We find another normal subgroup $R_{p^{m+1}}$ within the group $GL(2, p^{m+1})$ with $m \in \mathbb{N}$ if we look at the kernel of the reduction map modulo p^m ,

$$R_{p^{m+1}} = \{ A \in \operatorname{GL}(2, p^{m+1}) \mid A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p^m \}.$$
(5.2)

Proposition 5.1.4.

 $R_{p^{m+1}}$ is an abelian normal subgroup of $GL(2, p^{m+1})$ of size p^4 and exponent p. We get the exact sequence of groups

$$1 \to R_{p^{m+1}} \to \operatorname{GL}(2, p^{m+1}) \to \operatorname{GL}(2, p^m) \to 1.$$

Proof.

Being the kernel of the reduction map, $R_{p^{m+1}}$ is a normal subgroup. The map

$$\begin{array}{ccc} \mathbf{M}(2,p) \to & R_{p^{m+1}} \\ \mathbf{A} & \mapsto 1 + p^m \tilde{A} \end{array}$$

is an isomorphism from the additive group M(2, p) of 2×2 -matrices with entries modulo p onto $R_{p^{m+1}}$, if \hat{A} denotes any matrix in $GL(2, p^{m+1})$ whose reduction modulo p is equal to A. Knowing the additive structure of M(2, p)we conclude that the group $R_{p^{m+1}}$ is abelian, of exponent p and of size p^4 .

We can identify the elements of the factor group $GL(2, p^{m+1})/R_{p^{m+1}}$ with matrices having entries modulo p^m . Since matrix multiplication is compatible with reduction, we get an isomorphism of groups onto $GL(2, p^m)$. П

We get further normal subgroups of $GL(2, p^m)$ for $m \ge 2$ if we take intersections of those we have already determined. In particular, we find

$$D_{p^m} = R_{p^m} \cap \operatorname{SL}(2, p^m) \quad \text{with } |D_{p^m}| = p^3,$$

$$Z_{p^m} = R_{p^m} \cap Z(\operatorname{GL}(2, p^m)) \quad \text{with } |Z_{p^m}| = p.$$
(5.3)

Proposition 5.1.5.

For prime numbers $p \neq 2$ and $m \geq 2$ we have $R_{p^m} = D_{p^m} \times Z_{p^m}$.

Proof.

Using the statements in (5.3) we only have to show that $D_{p^m} \cap Z_{p^m} = 1$. Any matrix in $D_{p^m} \cap Z_{p^m}$ has the form $\binom{a \ 0}{0 \ a}$ with $a^2 \equiv 1 \mod p^m$ and $a \equiv 1 \mod p^{m-1}$. If we represent $a \in (\mathbb{Z}/p^m\mathbb{Z})^*$ by $a = 1 + bp^{m-1}$ with $0 \leq b < p$, the formula

$$1 \equiv (1 + bp^{m-1})^2 \equiv 1 + 2bp^{m-1} \bmod p^m$$

provides the result b = 0 for $p \neq 2$, which is the assertion.

When p = 2, however, the situation is quite different. We conclude from the preceding that $Z_{2^m} \leq D_{2^m}$. We consider instead the following subgroups of $R_{2^{m+1}}$ for $m \in \mathbb{N}$

$$V_{2^{m+1}} = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2^{m+1} & 0 \\ 0 & 2^{m+1} \end{pmatrix}, \begin{pmatrix} 2^{m+1} & 2^{m} \\ 2^{m} & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2^{m} \\ 2^{m} & 2^{m+1} \end{pmatrix} \}, W_{2^{m+1}} = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2^{m} \\ 2^{m} & 1 \end{pmatrix}, \begin{pmatrix} 2^{m+1} & 2^{m} \\ 0 & 2^{m+1} \end{pmatrix}, \begin{pmatrix} 2^{m+1} & 0 \\ 2^{m} & 2^{m+1} \end{pmatrix} \}.$$
(5.4)

Proposition 5.1.6.

For all $m \geq 2$, the subgroups V_{2^m} and W_{2^m} are normal in $GL(2, 2^m)$, and we have the relations

(i) $Z_{2^m} \leq V_{2^m}$, (ii) $D_{2^m} = Z_{2^m} \times W_{2^m}$, (iii) $R_{2^m} = V_{2^m} \times W_{2^m}$.

Proof.

The assertions (i), (ii), (iii) are valid by (5.3) and (5.4). It remains to show that for $m \in \mathbb{N}$ the subgroups $V_{2^{m+1}}, W_{2^{m+1}}$ are normal in $\mathrm{GL}(2, 2^{m+1})$.

These subgroups are the images of the additive subgroups

$$V = \{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \}, W = \{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \}$$

of M(2,2) under the map $A \mapsto 1 + 2^m \tilde{A}$ as in the proof of Proposition 5.1.4. Conjugation of $V_{2^{m+1}}$ or $W_{2^{m+1}}$ by matrices from $GL(2, 2^{m+1})$ is traced back via this map to conjugation of V or W by matrices from GL(2,2). Then $V_{2^{m+1}}$ and $W_{2^{m+1}}$ prove to be normal because V and W are invariant under conjugation by matrices from GL(2,2).

The center of $\operatorname{GL}(2, p^m)$ and the kernel $\operatorname{SL}(2, p^m)$ of the determinant map have the intersection

$$I_{p^m} = \begin{cases} \{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\} & p \neq 2, m \in \mathbb{N} \text{ or } p^m = 4, \\ \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\} & p^m = 2, \\ \{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 2^{m-1}+1 & 0 \\ 0 & 2^{m-1}+1 \end{pmatrix}\} & p = 2, m \ge 3. \end{cases}$$
(5.5)

A normal subgroup of index 2 in $GL(2, p^m)$ is

$$L_{p^m} = \begin{cases} \{ A \in \mathrm{GL}(2, 2^m) \mid \det A \equiv 1 \mod 4 \} & p = 2, m \ge 2, \\ \{ A \in \mathrm{GL}(2, p^m) \mid \left(\frac{\det A}{p}\right) = 1 \} & p \ne 2. \end{cases}$$
(5.6)

If M and N are normal subgroups of a group G then the product MN is a normal subgroup of G as well. Based on this insight, we find additional normal subgroups in $GL(2, p^m)$ with $m \ge 2$.

The situation is much easier in the case of the groups GL(2, p) for prime numbers p since there are no reduction maps to produce normal subgroups.

Proposition 5.1.7.

- (a) $\operatorname{GL}(2,2) = \operatorname{PSL}(2,2) \cong \mathfrak{S}_3$.
- (b) $PSL(2,3) \cong \mathfrak{A}_4$.

(c) For prime numbers $p \ge 5$, PSL(2,p) is a simple group of size $\frac{p^3-p}{2}$.

Proof.

See [Hupp67, II. 6.13, 6.14].

In Figure 5.1 we find the essential normal subgroups of the groups GL(2, p). For p = 2 and p = 3, the diagram is complete. The subgroup

$$U_3 = \{ \pm \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \}$$

of GL(2,3) is as an abstract group isomorphic to the quaternion group. Further, we have

$$N_2 = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \}.$$

For prime numbers $p \ge 5$, we use the fact that PSL(2, p) is a simple group and infer with little effort that each normal subgroup N of GL(2, p) is either of the form N = M SL(2, p) or of the form N = M with some subgroup $M \le Z(GL(2, p))$. Hence, additional normal subgroups of GL(2, p) appear only at those places in Figure 5.1 which are indicated by the arcs.

Figure 5.2 is a survey of the normal subgroups of $\operatorname{GL}(2, p^m)$ we have determined so far, the connecting lines indicating inclusions. All normal subgroups contained in R_{p^m} are given, but in order to keep clarity, the diagrams are restricted to a selection of important normal subgroups. For example, the kernels of the reduction maps modulo p^k with $1 \leq k < m$ provide an additional chain of normal subgroups starting with R_{p^m} which is not included here.

It is known that every abstract finite group G can be interpreted as subgroup of a certain symmetric group \mathfrak{S}_k for some $k \in \mathbb{N}$. In particular, G is isomorphic to a subgroup of $\mathfrak{S}_{|G|}$. Having the later application in mind, it is important for us to determine a number k as small as possible, so that $\operatorname{GL}(2, p^m)$ can be realized as a subgroup of \mathfrak{S}_k .



Fig. 5.1. Normal Subgroups of GL(2, p)

Proposition 5.1.8.

For $m \in \mathbb{N}$, the groups $GL(2, p^m)$ and $PGL(2, p^m)$ can be realized as subgroups of the following symmetric groups

- GL(2, p^m) as a subgroup of $\mathfrak{S}_{p^{2(m-1)}(p^2-1)}$, - PGL(2, p^m) as a subgroup of $\mathfrak{S}_{p^{m-1}(p+1)}$.

Proof.

Using the interpretation (5.1) as the automorphism group of $(\mathbb{Z}/p^m\mathbb{Z})^2$, $\operatorname{GL}(2, p^m)$ permutes the elements of maximal order p^m of $(\mathbb{Z}/p^m\mathbb{Z})^2$, and different automorphisms induce different permutations. Since there are exactly $p^{2m} - p^{2(m-1)}$ elements of order p^m , we get the assertion.

PGL(2, p^m) permutes the cyclic subgroups of size p^m of $(\mathbb{Z}/p^m\mathbb{Z})^2$, and different elements of PGL(2, p^m) induce different permutations. Since each of these cyclic subgroups contains exactly $p^{m-1}(p-1)$ of a total amount of $p^{2m} - p^{2(m-1)}$ elements of order p^m , the number of these subgroups has to be equal to $p^{m-1}(p+1)$.

From the preceding proof we recognize using Proposition 5.1.2 that the number of cyclic subgroups of size n in $(\mathbb{Z}/n\mathbb{Z})^2$ is equal to $\psi(n)$ where

$$\psi(n) = n \prod_{p|n} (1 + \frac{1}{p}).$$
(5.7)

For $n \in \mathbb{N}$, the group $\operatorname{GL}(2, n)$ can therefore be realized as a subgroup of $\mathfrak{S}_{\varphi(n)\psi(n)}$ and the group $\operatorname{PGL}(2, n)$ as a subgroup of $\mathfrak{S}_{\psi(n)}$, respectively.



Fig. 5.2. Normal Subgroups of $\operatorname{GL}(2, p^m), m \ge 2$

5.2 Subfields of $k(E_n)$

For simplicity reasons we make the following restrictions in this section: Let k be an algebraic number field and E an elliptic curve defined over k without complex multiplication, i. e. with $\operatorname{End}(E) \cong \mathbb{Z}$. Let $n \in \mathbb{N}$, $n \geq 2$, be chosen appropriately so that the degree of the extension $k(E_n)/k$ is maximal, that is, E_n has rank 2 over \mathbb{Z} and $\operatorname{Gal}(k(E_n)/k)$ may be identified with $\operatorname{GL}(2, n)$ via $\overline{\varphi}_n$ (see (3.8)).

In most of the statements below we might weaken the requirements to $\operatorname{Aut}(E) = \pm 1$, or $j(E) \neq 0, 1728$, or the characteristic of the base field being prime to n. However, these generalizations will not be pursued any further in this place.

By the Main Theorem of Galois theory, the subgroups of $\operatorname{GL}(2, n)$ correspond to subfields of the torsion point extension $k(E_n)/k$. If a proper subgroup of $\operatorname{GL}(2, n)$ appears as Galois group of $k(E_n)/k$, some of the quantities, whose adjunction to k gives a certain subfield of $k(E_n)/k$, are in the given situation already contained in smaller subfields so that some of these subfields coincide. The above agreement on the Galois group constitutes therefore the most general case from which any other may be read off.

Each automorphism of $\operatorname{Gal}(\overline{k}/k)$ gets a geometric interpretation by its operation on E. In this section we mainly address the restriction of these automorphisms to $k(E_n)$. An automorphism $\sigma \in \operatorname{Gal}(k(E_n)/k)$ corresponds bijectively under the faithful representation $\overline{\varphi}_n$ to a module automorphism of E_n , surjectivity being assured by the above condition to n. Having chosen a module basis $\{P,Q\}$ of E_n , we can represent the automorphism σ by a matrix $A_{\sigma} = {a \atop c \atop d} \in \operatorname{GL}(2, n)$. After changing the module basis, σ corresponds to a matrix which is similar to A_{σ} .

From these observations we conclude that the fixed field belonging to a subgroup of GL(2, n) is only determined up to conjugation. At least we get a unique bijective relation between the normal subgroups of GL(2, n) and the Galois subfields of $k(E_n)/k$.

We intend to find a description of the torsion point fields which expresses the field under consideration as a composite of subfields having an easier or an already known structure.

Proposition 5.2.1.

Let $n = p_1^{m_1} \cdot \ldots \cdot p_r^{m_r}$ be the canonical prime factor decomposition of n. Assume $\operatorname{Gal}(k(E_n)/k) \cong \operatorname{GL}(2,n)$. Then $k(E_n)$ is the composite of the linear disjoint subfields $k(E_{p_i^{m_i}})$, i. e. we have

$$k(E_n) = k(E_{p_1^{m_1}}) \cdots k(E_{p_r^{m_r}})$$

and $k(E_{p_i^{m_i}}) \cap k(E_{p_j^{m_j}}) = k \text{ for } i \neq j$.

Proof.

By Proposition 3.4.1 (a) we conclude $E_n \cong E_{p_1^{m_1}} \times \ldots \times E_{p_r^{m_r}}$. Thus, we can

write every *n*-torsion point *P* as a linear combination of $p_i^{m_i}$ -torsion points P_i , and we can express the coordinates of *P* in rational terms of the coordinates of the P_i . $k(E_n)$ is therefore contained in the composite of the fields $k(E_{p_i^{m_i}})$.

By assumption we have $[k(E_n):k] = |\operatorname{GL}(2,n)|$, and the last quantity is equal to the product of the extension degrees $[k(E_{p_i^{m_i}}):k]$. Combining these statements, we recognize that $k(E_n)$ equals the composite of the $k(E_{p_i^{m_i}})$ and that the $k(E_{n_i^{m_i}})$ are linear disjoint from each other.

On the basis of Proposition 5.2.1 we may restrict our attention to torsion points of prime power order to determine the structure of certain subfields, whenever it is convenient. We obtain, however, the following results without making use of the simplification just mentioned.

Proposition 5.2.2.

- (a) For $m, n \in \mathbb{N}$ with $m \mid n$ we have $k(E_m) \subseteq k(E_n)$, and the corresponding fixed group is the kernel $\{A \in GL(2,n) \mid A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod m \}$ of the reduction map modulo m.
- (b) We have $k(\mu_n) \subset k(E_n)$, and the corresponding fixed group is SL(2, n).
- (c) We have $k(x(E_n)) \subset k(E_n)$, and the corresponding fixed group is $\{\pm 1\}$.

Proof.

Let $\{P, Q\}$ be a module basis of E_n . Let $\sigma \in \text{Gal}(k(E_n)/k)$ be represented by $A_{\sigma} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}(2, n)$ with respect to this basis.

(a) Let $n = h \cdot m$. Then $\{h \cdot P, h \cdot Q\}$ is a basis of E_m . If σ operates trivially on E_m , we conclude by applying A_{σ} to $h \cdot P$ and $h \cdot Q$ that we have $A_{\sigma} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod m$. Conversely, any $A \in \operatorname{GL}(2, n)$ satisfying $A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod m$ fixes the basis elements $h \cdot P$ and $h \cdot Q$, thus it fixes all of E_m .

(b) [Silv86, III. Cor. 8.1.1, V. Prop. 2.3]

By [Silv86, III. §8] there exists on E_n a bilinear, alternating, surjective, nondegenerate map $e_n : E_n \times E_n \to \mu_n$, called the *Weil pairing*, which is compatible with the operation of the absolute Galois group $\operatorname{Gal}(\overline{k}/k)$. Because of this compatibility every automorphism of $\operatorname{Gal}(\overline{k}/k)$ which fixes all elements of $k(E_n)$ also fixes all elements of μ_n . Hence we get $k(\mu_n) \subset k(E_n)$. With the above notations we have

$$\sigma(e_n(P,Q)) = e_n(aP + cQ, bP + dQ) = e_n(P,Q)^{ad-bc} = e_n(P,Q)^{\det A_\sigma}.$$

From this we conclude that σ operates on μ_n by $\zeta \mapsto \zeta^{\det A_{\sigma}}$ which is independent of any chosen basis. The fixed group corresponding to $k(\mu_n)$ is equal to SL(2, n).

(c) Any two points $P_1, P_2 \in E$ satisfy: $x(P_1) = x(P_2) \iff P_1 = \pm P_2$. The reason is that for any given x the equation $y^2 = x^3 + ax + b$ has no more than two solutions which have the form $\pm y$.

Let $\phi \in \operatorname{Aut}(E_n)$ operate trivially on the *x*-coordinates of all *n*-torsion points. Then we have $\phi(P) = \pm P$, $\phi(Q) = \pm Q$ and $\phi(P+Q) = \pm (P+Q)$, so ϕ corresponds to $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Conversely, $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ fixes all *x*-coordinates. \Box
The following statements on isogenies serve to determine the fixed field corresponding to the center Z(GL(2, n)). They may be found, for example, in [Silv86, III. 4.12, 4.13.1, 4.13.2].

- Given any finite additive subgroup U of E, there exists an elliptic curve E' defined over \overline{k} and a separable isogeny $\phi: E \to E'$ satisfying ker $(\phi) = U$.
- If U remains fixed as a set under the operation of $\operatorname{Gal}(\overline{k}/k)$, E' and ϕ can be chosen to be defined over k. The curve E' is uniquely determined up to k-isomorphisms and is called the quotient curve E/U. The j-invariant j(E/U) is an element of k.

The cyclic subgroups of size n of E_n can be viewed as the kernels of isogenies. In such a subgroup U every element remains fixed under the operation of $\operatorname{Gal}(\overline{k}/k(E_n))$. The curve E/U is therefore defined over $k(E_n)$. If we thus set

$$J_n = J_n(E) = \{ j(E/U) \mid U \le E_n, U \text{ cyclic }, |U| = n \}, \qquad (5.8)$$

we have $J_n \subset k(E_n)$. The size of J_n is at most equal to the number of cyclic subgroups of size n of E_n . Hence we have $|J_n| \leq \psi(n)$ with $\psi(n)$ as defined in (5.7).

Proposition 5.2.3.

We have $k(J_n) \subset k(E_n)$, and the corresponding fixed group is the center $Z(\operatorname{GL}(2,n))$.

Proof.

Let L be the fixed field corresponding to $Z(\operatorname{GL}(2,n))$. The matrices of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ with $a \in (\mathbb{Z}/n\mathbb{Z})^*$ fix all cyclic subgroups U of E_n of size n. Therefore, this also holds for $\operatorname{Gal}(k(E_n)/L)$ and $\operatorname{Gal}(\overline{k}/L)$. We conclude that all quotient curves E/U are defined over L and that we have $j(E/U) \in L$ which leads us to $k(J_n) \subseteq L$.

Any two subgroups U, V of size n in E_n satisfy: $E/U \cong E/V \iff U = V$. For if we let $\pi_U : E \to E/U$ and $\pi_V : E \to E/V$ denote the canonical isogenies and if $\psi : E/U \to E/V$ is an isomorphism, $\psi \circ \pi_U$ and π_V are isogenies $E \to E/V$ of degree n. From the assumption $\operatorname{End}(E) = \mathbb{Z}$ we conclude $\psi \circ \pi_U = \pm \pi_V$, and from the equality of the kernels we get U = V. The converse is obvious.

In particular, if we have $U \neq V$ for two cyclic subgroups of E_n of size n, we get $j(E/U) \neq j(E/V)$. Thus the quantities given in (5.8) are distinct, and we have $|J_n| = \psi(n)$.

Let U and V be cyclic subgroups of E_n of size n. Then there is a $\sigma \in \operatorname{Gal}(k(E_n)/k)$ satisfying $\sigma(U) = V$. We have $\sigma(E/U) \cong E/V$ since an isomorphism is given by $\pi_V \circ \sigma \circ \pi_U^{-1}$. On the other hand, σ operates on the coefficients of a defining equation of E/U so that we have

$$\sigma(j(E/U)) = j(\sigma(E/U)) = j(E/V).$$

All elements of J_n are therefore conjugate under $\operatorname{Gal}(k(E_n)/k)$, and the Galois group $\operatorname{Gal}(k(E_n)/k)$ permutes the cyclic subspaces of size n of E_n just like the corresponding j-invariants in J_n .

If $\sigma \in \text{Gal}(k(E_n)/k(J_n))$ then σ fixes all these subspaces, in particular given a module basis $\{P, Q\}$, σ fixes the three cyclic subspaces generated by P, Q, and P + Q, respectively. A_{σ} must therefore have the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ with $a \in (\mathbb{Z}/n\mathbb{Z})^*$ so that it is an element of the center. \Box

Now let $n = p^m$ be the power of a prime number, the notations of the normal subgroups being adopted from Section 5.1. From Proposition 5.2.2 and Proposition 5.2.3 we may already conclude:

- In the extension $k(E_{p^{m+1}})/k$, the normal subgroup $R_{p^{m+1}}$ corresponds to the subfield $k(E_{p^m})$.
- In the extension $k(E_{p^m})/k$, the fixed field corresponding to L_{p^m} is

Fix
$$(L_{p^m}) = \begin{cases} k(\sqrt{-1}), \text{ for } p = 2, m \ge 2\\ k(\sqrt{p^*}), \text{ for } p \ne 2, \end{cases}$$

using the symbol $p^* = (-1)^{\frac{p-1}{2}}p$. For $p \neq 2$ this is the unique quadratic subfield of $k(\mu_p)$.

- Because of the equality $I_{2^{m+1}} = \operatorname{SL}(2, 2^{m+1}) \cap Z(\operatorname{GL}(2, 2^{m+1}))$ the normal subgroup $I_{2^{m+1}}$ belongs to $k(J_{2^{m+1}}, \mu_{2^{m+1}})$.

Concerning prime numbers p, in general only the subfield $k(x(E_p))$ of $k(E_p)$ can be expressed as a composite of Galois subfields.

Proposition 5.2.4.

If p is a prime number, we have $k(x(E_p)) = k(\mu_p)k(J_p)$.

Proof.

For $p \ge 3$ the intersection of SL(2, p) and Z(GL(2, p)) is equal to $\{\pm 1\}$. In the case of p = 2 we have $k(E_2) = k(x(E_2)) = k(J_2)$.

Remark 5.2.1.

For $p \geq 5$, PSL(2, p) is a simple normal subgroup of PGL(2, p) of index 2 which is determined by the condition that the determinants of all matrices contained in its matrix classes are squares in \mathbb{F}_p^* . Thus the extension $k(J_p)/k(\sqrt{p^*})$ does not have any Galois intermediate field.

The essential Galois subfields of the extension $k(E_p)/k$ for prime numbers $p \geq 5$ can be found in Figure 5.3. By the above remark, additional Galois subfields only appear at the places indicated by the arcs.



Fig. 5.3. Galois Correspondence of $k(E_p)/k$ for $p \ge 5$

If we consider proper prime powers $n = p^{m+1}$, we can describe the extension $k(E_{p^{m+1}})/k$ by means of the subextension $k(E_{p^m})/k$. More precisely, we have the following proposition.

Proposition 5.2.5.

(a) If $p \neq 2$ is a prime number and $m \in \mathbb{N}$, we have

$$k(E_{p^{m+1}}) = k(E_{p^m})k(\mu_{p^{m+1}})k(J_{p^{m+1}}).$$

(b) If $m \in \mathbb{N}$ and $M_{2^{m+1}}$ is the fixed field corresponding to $\pm W_{2^{m+1}}$, we have

$$k(E_{2^{m+1}}) = k(E_{2^m})k(\mu_{2^{m+1}})k(J_{2^{m+1}})M_{2^{m+1}}.$$

Proof.

For all prime numbers p, the fixed group of $k(E_{p^m})k(\mu_{p^{m+1}})k(J_{p^{m+1}})$ is equal to the intersection

$$R_{p^{m+1}} \cap \operatorname{SL}(2, p^{m+1}) \cap Z(\operatorname{GL}(2, p^{m+1})) = \begin{cases} \{\binom{1}{0} \\ 0 \end{bmatrix}, & p \neq 2 \\ \{\binom{1}{0} \\ 0 \end{bmatrix}, \begin{pmatrix} 2^{m+1} \\ 0 \\ 2^{m+1} \end{pmatrix}\}, & p = 2 \end{cases}$$

In the case of $p \neq 2$ this is already the assertion of the proposition. In the case of p = 2 the matrix $\binom{2^m+1}{0}{2^m+1}$ is not an element of $\pm W_{2^{m+1}}$, from which we may deduce the assertion.

The intermediate fields which result from the discussion in this section are summarized in Figure 5.4 and Figure 5.5. The special cases $p^m = 2, 3, 4$ which have not yet been covered are dealt with separately in Section 5.4 and Section 5.5.





Fig. 5.4. Galois Correspondence of $k(E_{p^m})/k$ for $p \ge 3$ and $m \ge 2$



Fig. 5.5. Galois Correspondence of $k(E_{2^m})/k$ for $m \ge 3$

5.3 Defining Polynomials of Subfields of $k(E_n)$

Hitherto, we have identified the subfields K of the extension $k(E_n)/k$ by their corresponding fixed groups. These fields, however, can also be described by defining polynomials:

- In the case of a general algebraic extension K/k we use the minimal polynomial of some primitive element of K over k.
- In the case of a Galois extension K/k we may use instead some polynomial in k[X] whose splitting field is equal to K. The degree of such a polynomial is usually much smaller than the degree of a minimal polynomial.

Frequently we are in the situation that we have a chain L/K/k of extensions of number fields and already know defining polynomials for the subextensions L/K and K/k. If we want to determine a defining polynomial of L/k, we proceed by the the following strategy (see [Cohe93, 3.6.2, Alg. 3.6.4] or [Tra76]):

Let θ be a primitive element of K over k and ϑ a primitive element of L over K. Let $P(X) \in K[X]$ be the minimal polynomial of ϑ over K and $R(X) \in k[X]$ the respective one of θ over k. If $N_{K/k}$ denotes the norm map extended to the respective polynomial rings,

$$Q(X) = N_{K/k}(P)(X) \in k[X]$$

is the power of an irreducible polynomial having the zero ϑ . Consequently, if Q(X) does not possess repeated factors, Q(X) is a defining polynomial for L/k. We can always achieve Q(X) being squarefree if we possibly replace P(X) by the polynomial $P(X - m\theta)$ with a suitable value for $m \in \mathbb{Z}$. If we write

$$P(X) = \sum_{i=0}^{n} u_i X^i \quad \text{with} \quad u_i \in K$$

and express the coefficients u_i in the form $u_i = g_i(\theta)$ with $g_i(X) \in k[X]$, let us define

$$\tilde{P}(X,Y) = \sum_{i=0}^{n} g_i(Y) X^i.$$

We have introduced these notations to calculate Q(X) as follows:

$$Q(X) = \operatorname{Res}_Y(R(Y), P(X - mY, Y)),$$

i. e. as a resultant with respect to the variable Y.

In the case of Galois extensions we have a much simpler principle: If we are given two Galois subfields as splitting fields of the polynomials P(X) and Q(X), respectively, the composite of these fields is the splitting field of the polynomial P(X)Q(X).

These procedures are to be applied to already known subfields of our torsion point extensions. We get:

- $-k(J_n)$ is defined by the *n*-th modular polynomial $\Phi_n(X, j(E))$.
 - The calculation of $\Phi_n(X, Y)$ for general n can be reduced by resultants to the calculation of $\Phi_p(X, Y)$ for all prime numbers p (cf. [Cox89, Prop. 13.14] or [Web08, §69]).

 $\Phi_n(X, Y)$ has integral coefficients and is of degree $\psi(n)$ in X. Additional properties of $\Phi_n(X, Y)$ can be found for example in [Cox89, Thm. 11.18]. - $k(\mu_n)$ is defined by the *n*-th cyclotomic polynomial

$$\phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)},$$

where μ denotes the Möbius-function.

- $\phi_n(X)$ has integral coefficients and is of degree $\varphi(n)$.
- $-k(x(E_n))$ can be defined by $A_n(X, Y)$ as in Section 3.3. Since the points of E_n whose order is smaller than n can be expressed rationally by the points of order n, we can restrict ourselves to the x-coordinates of the points of order n, and similar to $\phi_n(X)$ we obtain as a defining polynomial

$$\Lambda_n(X) = \prod_{d|n} A_d(X, Y)^{\mu(n/d)}$$

For $n \geq 3$ the variable Y does not appear in $\Lambda_n(X)$, and in the case of n = 2 we set $\Lambda_2(X) = 2(X^3 + aX + b)$.

 $\Lambda_n(X)$ is a polynomial of degree $\frac{1}{2}\varphi(n)\psi(n)$ with leading coefficient equal to p, if n is a power of p, or equal to 1, if n has at least two different prime divisors.

 $-k(E_n)$ arises from $k(x(E_n))$ by adjoining the *y*-coordinate of one point of order *n*. We are therefore able to apply the procedure described above and calculate the defining polynomial

$$T_n(X) = \text{Res}_Y(\Lambda_n(Y), X^2 - (Y^3 + aY + b)).$$

Using the remark above concerning composites, we obtain in the case of $n = p^m$ defining polynomials for the following subextensions.

- $-k(E_{p^m}, \mu_{p^{m+1}})$ is given by the polynomial $\Lambda_{p^m}(X) \phi_{p^{m+1}}(X)$.
- $-k(E_{p^m}, J_{p^{m+1}})$ is given by the polynomial $\Lambda_{p^m}(X) \Phi_{p^{m+1}}(X, j(E))$.
- $-k(J_{2m+1}, \mu_{2m+1})$ is given by the polynomial $\Phi_{2m+1}(X, j(E)) \phi_{2m+1}(X)$.

The results of these considerations are summarized in Table 5.1.

From the assumption $\operatorname{Gal}(k(E_n)/k) \cong \operatorname{GL}(2,n)$ we conclude that the polynomials $\phi_n(X)$, $\Phi_n(X, j(E))$ and $\Lambda_n(X)$ are necessarily irreducible over k[X].

Normal Subgrp.	Fixed Field	Degree over k	Defining Polynomial
$\operatorname{GL}(2,n)$	k	1	X
$\operatorname{SL}(2,n)$	$k(\mu_n)$	arphi(n)	$\phi_n(X)$
$Z(\operatorname{GL}(2,n))$	$k(J_n)$	$n\psi(n)arphi(n)$	$\Phi_n(X, j(E))$
±1	$k(x(E_n))$	$\frac{1}{2}n\psi(n)\varphi^2(n)$	$\Lambda_n(X)$
1	$k(E_n)$	$n\psi(n)arphi^2(n)$	$T_n(X)$
L_{p^m}	$k(\sqrt{p^*})$	2	$x^2 - p^*$
$R_{p^{m+1}}$	$k(E_{p^m})$	$p^{4m}(p^2-1)(p^2-p)$	$\Lambda_{p^m}(X)$
$D_{p^{m+1}}$	$k(E_{p^m},\mu_{p^{m+1}})$	$p^{4m+1}(p^2-1)(p^2-p)$	$\Lambda_{p^m}(X) \phi_{p^{m+1}}(X)$
$Z_{p^{m+1}}$	$k(E_{p^m}, J_{p^{m+1}})$	$p^{4m+3}(p^2-1)(p^2-p)$	$\Lambda_{p^m}(X) \Phi_{p^{m+1}}(X, j(E))$
$I_{2^{m+1}}$	$k(J_{2^{m+1}},\mu_{2^{m+1}})$	$2^{4m+3} \cdot 3$	$\Phi_{2^{m+1}}(X, j(E)) \phi_{2^{m+1}}(X)$

Table 5.1. Galois Subfields of $k(E_n)/k$

We finish this section by listing some important intermediate fields of $k(E_n)/k$ for $n \geq 3$ which are not Galois so that if we are given a subgroup of GL(2, n), the corresponding fixed field is only determined up to conjugation. These extensions are constructed by adjoining the x- and y-coordinate or only the x-coordinate of one point P of E_n of order n, by adjoining single j-invariants $j(E/\langle P \rangle)$ in J_n or by combining these processes.

In order to describe the corresponding fixed groups, we fix some point P which is our considered point or some generator of our considered cyclic subgroup and add some point Q to get a $\mathbb{Z}/n\mathbb{Z}$ -module basis $\{P, Q\}$ of E_n . In this way we get the subgroups of GL(2, n) which are given in Table 5.2 together with the additional information on the subfields.

We are able to compute minimal polynomials for the combined extension fields by the procedure described above. They are calculated by resultants in the polynomials Λ_n and Φ_n or T_n and Φ_n , respectively. These polynomials, however, are not irreducible in the respective subextensions, so we have to determine the correct irreducible factors to obtain defining polynomials. Since these polynomials are not required in the sequel, we will not continue to pursue their calculation.

Subgroup	Fixed Field	Degree over k	Defining	Number of
			Polynomial	Conjugate Subgroups
$\begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$	$k(P, j(E/\langle Q\rangle))$	$n\psi(n)\varphi(n)$		$n\psi(n)$
$\pm \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$	$k(x(P), j(E/\langle Q \rangle))$	$\frac{1}{2}n\psi(n)\varphi(n)$		$n\psi(n)$
$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$	k(P)	$\psi(n) \varphi(n)$	$T_n(X)$	$\psi(n)$
$\pm \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$	k(x(P))	$\frac{1}{2}\psi(n)\varphi(n)$	$\Lambda_n(X)$	$\psi(n)$
$\binom{*}{0} \binom{*}{*}$	$k(j(E/\langle P \rangle))$	$\psi(n)$	$\Phi_n(X, j(E))$	$\psi(n)$

Table 5.2. Non-Galois Subfields of $k(E_n)/k$ for $n \ge 3$

5.4 Decomposition in 2- and 3-Torsion Point Fields

Throughout this section, let k be an algebraic number field and E an elliptic curve defined over k, given by the equation $y^2 = x^3 + ax + b$ with discriminant $\Delta = -16(4a^3 + 27b^2)$ and j-invariant $j = -2^{12}3^3a^3/\Delta$.

We restrict ourselves to examine the decomposition behaviour only for unramified prime ideals. Doing this, we lose at most finitely many prime ideals. The Criterion of Néron, Ogg, Shafarevich determines exactly which prime ideals are excluded by our restriction.

Proposition 5.4.1. (Néron, Ogg, Shafarevich)

Let E be an elliptic curve defined over k, and let \mathfrak{p} be prime ideal of k having the norm q. Then the following assertions are equivalent:

(a) E has good reduction modulo p.

(b) \mathbf{p} is unramified in $k(E_n)/k$ for all $n \in \mathbb{N}$ with (n,q) = 1.

Proof.

See [Silv86, VII. 7.1].

Thus, if \mathfrak{p} is a prime ideal which does not divide n and which satisfies $v_{\mathfrak{p}}(\Delta) = 0$ for the normalized \mathfrak{p} -adic exponential valuation $v_{\mathfrak{p}} : k^* \to \mathbb{Z}, \mathfrak{p}$ is unramified in the extension $k(E_n)/k$.

When describing the decomposition laws we assume that the Galois group of the considered extension $k(E_n)/k$ is maximal, hence isomorphic to GL(2, n). This situation actually appears if E does not have complex multiplication over k (see Proposition 3.5.2). In the most general case the Galois group in question is a subgroup of GL(2, n) whose distinction includes a case by case study which gets more extensive as n increases. As an example we give here the possible Galois groups of the extension $k(E_2)/k$.

Proposition 5.4.2.

The Galois group of the extension $k(E_2)/k$ has one of the following forms:

$$\operatorname{Gal}(k(E_2)/k) \cong \begin{cases} \operatorname{GL}(2,2), & \text{if } \Delta \notin k^{*2} \text{ and } E_2(k) = \{\mathbf{0}\}, \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } \Delta \in k^{*2} \text{ and } E_2(k) = \{\mathbf{0}\}, \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } \Delta \notin k^{*2} \text{ and } E_2(k) \neq \{\mathbf{0}\}, \\ \{1\}, & \text{if } \Delta \in k^{*2} \text{ and } E_2(k) \neq \{\mathbf{0}\}. \end{cases}$$

Proof.

 $k(\sqrt{\Delta})$ is the subfield of $k(E_2)/k$ which is obtained by adjoining the discriminant of the defining polynomial $\Lambda_2(X) = 2(X^3 + aX + b)$. We have $[k(\sqrt{\Delta}):k] = 2$ if and only if Δ is no square in k^* . Since the *y*-coordinate of any 2-torsion point equals 0, $\Lambda_2(X)$ is irreducible over k[X] if and only if E has no k-rational 2-torsion point $\neq 0$.

From the next proposition we derive the important result that the splitting field of $X^3 - \Delta$ is a subfield of $k(E_3)$.

Proposition 5.4.3.

We have $k(\sqrt[3]{\Delta}, \mu_3) \subset k(x(E_3)), U_3 = \{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \pm \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}\}$ being the corresponding fixed group.

Proof. (cf. [Renn89, 3.1, Lemma 15]) If $P(X) = X^4 - s_1 X^3 + s_2 X^2 - s_3 X + s_4$ is a general polynomial of degree 4, its *cubic resolvent* is given by

$$R(X) = X^3 - s_2 X^2 + (s_1 s_3 - 4 s_4) X - (s_1^2 s_4 + s_3^2 - 4 s_2 s_4) .$$

By applying this formula to a defining polynomial of $k(x(E_3))/k$ in the shape $P(X) = X^4 + 18 a X^2 + 108 b X - 27 a^2$ (compare to $A_3(X)$ in Section 3.3) we calculate $R(X) = X^3 - 18 a X^2 + 108 a^2 X - 11664 b^2 - 1944 a^3$ being the cubic resolvent of P(X), and after substituting $X \mapsto -3X + 6a$ and cancelling the factor -27 we obtain

$$\tilde{R}(X) = X^3 + 16 \left(4 \, a^3 + 27 \, b^2\right) = X^3 - \Delta$$

as a defining polynomial for the subfield given by the cubic resolvent. $k(\sqrt[3]{\Delta}, \mu_3)$ is therefore contained in $k(x(E_3))$.

Because of $[k(\sqrt[3]{\Delta}, \mu_3) : k] = 6$ the only possible fixed group is the unique normal subgroup U_3 of size 8 in GL(2, 3).



Fig. 5.6. Galois Subfields of $k(E_2)/k$ and $k(E_3)/k$

In Section 5.1 we have determined all normal subgroups of the groups GL(2,2) and GL(2,3) and listed them in Figure 5.1. The corresponding Galois subfields of $k(E_2)/k$ or $k(E_3)/k$, respectively, are presented in Figure 5.6.

Now we describe the decomposition laws of the 2- and 3-torsion point fields. Figure 5.6 suggests to describe the decomposition law of the extensions $k(E_2)/k$ and $k(E_3)/k$ by stepping through the given subfields.

The decomposition law is known in $k(\sqrt{\Delta})/k$ (cf. Theorem 2.2.5). We obtain the decomposition in the subextension $k(E_2)/k(\sqrt{\Delta})$ in terms of the coefficients a_q in their interpretation as numbers of \mathbb{F}_q -rational points of the curve \tilde{E} reduced modulo q (see (3.12)).

Proposition 5.4.4.

Let *E* be an elliptic curve defined over *k* having the discriminant $\Delta \neq 0$. Assume $E_2(k) = \{\mathbf{0}\}$, *i.* e. $\operatorname{Gal}(k(E_2)/k(\sqrt{\Delta})) \cong \mathbb{Z}/3\mathbb{Z}$. Let \mathfrak{p} be a prime ideal of $k(\sqrt{\Delta})$ with the norm *q* satisfying (q, 2) = 1 and $v_{\mathfrak{p}}(\Delta) = 0$. Then \mathfrak{p} is fully decomposed in $k(E_2)/k(\sqrt{\Delta})$ if and only if $a_q \equiv 0 \mod 2$.

Proof. (cf. [Ito82, Theorem])

By (3.13), a_q is even if and only if $\#\tilde{E}_2(\mathbb{F}_q)$ is even. This is the case if and only if the polynomial $\Lambda_2(X) = 2(X^3 + aX + b)$ has a linear factor over $\mathbb{F}_q[X]$. By the Propositions 2.1.1 and 2.1.2 and by assumption, $f_{k(E_2)/k(\sqrt{\Delta})}(\mathfrak{p})$ is a divisor of the degree $[k(E_2): k(\sqrt{\Delta})] = 3$, so by Theorem 2.1.1 we infer that \mathfrak{p} is fully decomposed if and only if $\Lambda_2(X)$ has a linear factor in $\mathbb{F}_q[X]$. \Box

When stating further results, we use the *n*-th power residue symbol $\left(\frac{a}{\mathfrak{b}}\right)_n$ as described in (2.5) which is only defined if *k* contains μ_n , otherwise the ideal \mathfrak{b} of *k* is required to be the norm of some ideal in $k(\mu_n)$. If \mathfrak{p} is a prime ideal of *k* then $\left(\frac{a}{\mathfrak{p}}\right)_n$ characterizes the decomposition of \mathfrak{p} in $k(\sqrt[n]{a})/k$.

If we put together the obtained information and take into account the structure of the Galois group as described in Proposition 5.4.2, the decomposition law of 2-torsion point fields reads as follows.

Proposition 5.4.5. (Decomposition Law for 2-Torsion Point Fields) Let *E* be an elliptic curve over *k* having the discriminant $\Delta \neq 0$, and assume $\operatorname{Gal}(k(E_2)/k) \cong \operatorname{GL}(2,2)$. Let \mathfrak{p} be a prime ideal of *k* with the norm *q* such that (q,2) = 1 and $v_{\mathfrak{p}}(\Delta) = 0$. Then we have

$$f_{k(E_2)/k}(\mathfrak{p}) = \begin{cases} 1, & \text{if} \quad \left(\frac{\Delta}{\mathfrak{p}}\right)_2 = 1 & \text{and} \ a_q \equiv 0 \mod 2, \\ 3, & \text{if} \quad \left(\frac{\Delta}{\mathfrak{p}}\right)_2 = 1 & \text{and} \ a_q \equiv 1 \mod 2, \\ 2, & \text{if} \quad \left(\frac{\Delta}{\mathfrak{p}}\right)_2 = -1. \end{cases}$$

Proof.

The result is a consequence of Proposition 5.4.4. A fourth alternative does not appear in the above case distinction because GL(2,2) has no element of order 6. In particular, we have:

$$\left(\frac{\Delta}{\mathfrak{p}}\right)_2 = -1 \text{ implies } a_{q^2} \equiv a_q \equiv 0 \mod 2.$$

We let $k_{\Delta,3} = k(\sqrt[3]{\Delta}, \mu_3)$ denote the splitting field of $X^3 - \Delta$ over k. The prime decomposition in the subextension $k_{\Delta,3}/k$ of $k(E_3)/k$ is obtained by applying Theorem 2.2.5. We may again characterize the complete extension by means of the coefficients a_q in their interpretation as traces of the Frobenius automorphism, see (3.14).

Proposition 5.4.6. (Decomposition Law for 3-Torsion Point Fields) Let *E* be an elliptic curve over *k* having the discriminant $\Delta \neq 0$, and assume $\operatorname{Gal}(k(E_3)/k) \cong \operatorname{GL}(2,3)$. Let \mathfrak{p} be a prime ideal of *k* with the norm *q* which satisfies (q,3) = 1 and $v_{\mathfrak{p}}(\Delta) = 0$. Then

$$f_{k_{\Delta,3}/k}(\mathfrak{p}) = \begin{cases} 1, & \text{if} \quad q \equiv 1 \mod 3 \quad \text{and} \quad \left(\frac{\Delta}{\mathfrak{p}}\right)_3 = 1, \\ 3, & \text{if} \quad q \equiv 1 \mod 3 \quad \text{and} \quad \left(\frac{\Delta}{\mathfrak{p}}\right)_3 \neq 1, \\ 2, & \text{if} \quad q \equiv 2 \mod 3. \end{cases}$$

If \mathfrak{P} is a prime ideal in $k_{\Delta,3}$ with $v_{\mathfrak{P}}(\Delta) = 0$ whose norm q' satisfies (q',3) = 1, we have

$$f_{k(E_3)/k_{\Delta,3}}(\mathfrak{P}) = \begin{cases} 1, & \text{if} \quad a_{q'} \equiv 2 \mod 3, \\ 2, & \text{if} \quad a_{q'} \equiv 1 \mod 3, \\ 4, & \text{if} \quad a_{q'} \equiv 0 \mod 3. \end{cases}$$

Proof.

The first term is implied directly by Proposition 2.2.1 and Theorem 2.2.5. For $q \equiv 2 \mod 3$ we observe

$$\left(\frac{\underline{A}}{\overline{\mathfrak{p}}}\right)_{3} \equiv \underline{A}^{\frac{q^{2}-1}{3}} \equiv \underline{A}^{\frac{q+1}{3}(q-1)} \equiv 1 \bmod \mathfrak{p}.$$

The second formula can be read off from the matrices of the fixed group U_3 (see Proposition 5.4.3) if we notice that $a_{q'}$ modulo 3 gives the trace of the Frobenius automorphism belonging to \mathfrak{P} .

Using Proposition 5.4.6 we may explicitly write down the general decomposition law in $k(E_3)/k$ for unramified prime ideals, where we have to disregard those finitely many prime ideals which divide 3 or appear in Δ .

Let now the base field be $k = \mathbb{Q}$, and let E be an elliptic curve defined over \mathbb{Q} . We identify the elements of $\operatorname{Gal}(\mathbb{Q}(E_3)/\mathbb{Q})$ with their corresponding matrices in $\operatorname{GL}(2,3)$. As we know how any given prime number $p \neq 3$ with $v_p(\Delta) = 0$ decomposes in $\mathbb{Q}(E_3)/\mathbb{Q}$, we can perform the complementary task to characterize the set of prime numbers whose respective Frobenius automorphisms belong to a given conjugacy class C of $\operatorname{GL}(2,3)$. The result of this calculation is summarized in Table 5.3.

Element	Necessary Conditions for			Order in			
of C	$\left(\frac{\mathbb{Q}(E_3)/\mathbb{Q}}{p}\right) \in C$			$\mathbb{Q}(\mu_3)$	$\mathbb{Q}(\sqrt[3]{\Delta},\mu_3)$	$\mathbb{Q}(x_3)$	$\mathbb{Q}(E_3)$
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$p \equiv 1 (3) \angle $	$\Delta^{\frac{p-1}{3}} \equiv 1(p)$	$a_p \equiv 2 (3)$	1	1	1	1
$\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)$	$p \equiv 1 (3) \angle $	$\Delta^{\frac{p-1}{3}} \equiv 1(p)$	$a_p \equiv 1 (3)$	1	1	1	2
$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$p \equiv 1 (3) \angle $	$\Delta^{\frac{p-1}{3}} \not\equiv 1\left(p\right)$	$a_p \equiv 2 (3)$	1	3	3	3
$\begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}$	$p \equiv 1 (3)$	$\Delta^{\frac{p-1}{3}} \not\equiv 1\left(p\right)$	$a_p \equiv 1 (3)$	1	3	3	6
$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$p \equiv 2 (3)$		$a_p \equiv 0 (3)$	2	2	2	2
$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$p \equiv 1 (3)$ \angle	$\Delta^{\frac{p-1}{3}} \equiv 1(p)$	$a_p \equiv 0 (3)$	1	1	2	4
$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$	$p \equiv 2 (3)$		$a_p \equiv 2 (3)$	2	2	4	8
$\begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}$	$p \equiv 2 (3)$		$a_p \equiv 1 (3)$	2	2	4	8

Table 5.3. Decomposition in $\mathbb{Q}(E_3)/\mathbb{Q}$

Each row of Table 5.3 corresponds to a conjugacy class C of GL(2, 3). One representative is given for each class C, and we state necessary (and in this case also sufficient) conditions for a Frobenius automorphism to be a member of C. In addition, we list the orders of the elements of C in the Galois groups of the respective normal subextensions of $\mathbb{Q}(E_3)/\mathbb{Q}$.

The decomposition law for 3-torsion point fields over \mathbb{Q} was already stated in [Renn89, 2, Theorem 14] for fully decomposed prime numbers in terms of the coefficients a_p .

5.5 Decomposition in 4-Torsion Point Fields

As before, let *E* be an elliptic curve defined over the number field *k* satisfying an equation $y^2 = x^3 + ax + b$ with discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$.

Considering the 4-torsion point fields, we are still in a situation which is simpler than the case of general *n*-torsion point extensions because similar to the cases of 2- and 3-torsion point fields, the splitting field $k_{\Delta,4} = k(\sqrt[4]{\Delta}, \mu_4)$ of the polynomial $X^4 - \Delta$ over k is contained in $k(E_4)$. We continue to assume, however, that $\operatorname{Gal}(k(E_4)/k) \cong \operatorname{GL}(2,4)$, and in this case, $k_{\Delta,4}$ is not contained in $k(x(E_4))$.

Proposition 5.5.1.

We have $k_{\Delta,4} \subset k(E_4)$. The corresponding fixed group is

$$H = \left\{ \begin{array}{c} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 2 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \\ \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix} \right\}.$$

Proof.

In [LaTr76, III, §11, p. 218ff.] we find an explicit construction of $\sqrt[4]{\Delta}$ by the coordinates of the 4-torsion points. Since we have $[k_{\Delta,4}:k] = 8$ and H is the only normal subgroup of size 12 in GL(2,4), H is the fixed group we are looking for.

The result of this proposition cannot be generalized automatically to torsion point extensions $k(E_n)/k$ since the splitting field $k_{\Delta,n}$ of $X^n - \Delta$ over kis in general not contained in $k(E_n)$. If we look at n = p for prime numbers pwe do not even find a normal subgroup of the appropriate size within the Galois group $\text{Gal}(k(E_p)/k)$, and in the cases n = 8 and n = 9 we are able to give counterexamples.

Figure 5.7 presents all Galois subfields of the extension $k(E_4)/k$. Using the results of Section 5.4 and Theorem 2.2.5, we can state the decomposition law of the subfield $F = k(E_2)k_{\Delta,4}$.

Proposition 5.5.2.

Let E be an elliptic curve over k with discriminant $\Delta \neq 0$, and assume $\operatorname{Gal}(k(E_4)/k) \cong \operatorname{GL}(2,4)$. Let \mathfrak{p} be a prime ideal of k with the norm q which satisfies (q,2) = 1 and $v_{\mathfrak{p}}(\Delta) = 0$. Then

$$f_{k_{\Delta,4}/k}(\mathfrak{p}) = \begin{cases} 1, \ if \quad q \equiv 1 \mod 4 \ and \ \left(\frac{\Delta}{\mathfrak{p}}\right)_4 = 1, \\ 2, \ if \quad q \equiv 1 \mod 4 \ and \ \left(\frac{\Delta}{\mathfrak{p}}\right)_4 = -1 \\ or \quad q \equiv 3 \mod 4, \\ 4, \ if \quad q \equiv 1 \mod 4 \ and \ \left(\frac{\Delta}{\mathfrak{p}}\right)_4 \neq \pm 1. \end{cases}$$

If \mathfrak{P} is a prime ideal in $k_{\Delta,4}$ with $v_{\mathfrak{P}}(\Delta) = 0$ whose norm q' satisfies (q',2) = 1, we have

$$f_{F/k_{\Delta,4}}(\mathfrak{P}) = \begin{cases} 1, & \text{if} \quad a_{q'} \equiv 2 \mod 4, \\ 3, & \text{if} \quad a_{q'} \equiv 3 \mod 4. \end{cases}$$

Proof.

The first term results from Proposition 2.2.1 and Theorem 2.2.5. In the case of $q \equiv 3 \mod 4$ we have

$$\left(\frac{\Delta}{\mathfrak{p}}\right)_4 \equiv \Delta^{\frac{q^2-1}{4}} \equiv \Delta^{\frac{q+1}{4}(q-1)} \equiv 1 \mod \mathfrak{p}.$$

The second formula results from the fixed group H in Proposition 5.5.1. \Box

The elements of $\operatorname{Gal}(k(E_4)/F) = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 2 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix} \}$ cannot be distinguished by using only the coefficients a_q and the quantities used in the statement of Proposition 5.5.2.



Fig. 5.7. Galois Correspondence of $k(E_4)/k$

In order to state the decomposition law of $k(E_4)/k$, we will make use of the intermediate field L (see Figure 5.7). The fixed group corresponding to Lis $V_4 = \{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}\}$. To perform the missing step, we will observe the decomposition of a defining polynomial of L and then apply Theorem 2.1.1. Since the factor group Gal(L/k) of $\text{Gal}(k(E_4)/k)$ is isomorphic to \mathfrak{S}_4 as an abstract group, we can hope to find a polynomial of degree 4 whose splitting field over k is equal to L.

By means of invariant theoretic methods described in the next chapter we calculate as an appropriate polynomial (see (6.6))

 $B(X) = X^4 - 4\Delta X - 12a\Delta$ with discriminant $\text{Dis}(B) = 2^{12}3^6b^2\Delta^3$.

The decomposition type of the polynomial B(X) with respect to the prime ideal \mathfrak{p} of k with the norm q is defined as the list of the degrees of the irreducible factors of B(X) in the residue field \mathbb{F}_q , sorted by decreasing size.

The decomposition law for $k(E_4)/k$ is then obtained by combining all information achieved so far with the assertion of Theorem 2.1.1 applied to the polynomial B(X).

Proposition 5.5.3. (Decomposition Law for 4-Torsion Point Fields) Let *E* be an elliptic curve defined over *k* with discriminant $\Delta \neq 0$, and assume $\operatorname{Gal}(k(E_4)/k) \cong \operatorname{GL}(2,4)$. Let \mathfrak{p} be a prime ideal of *k* with the norm *q* which satisfies (q, 6) = 1, $v_{\mathfrak{p}}(\Delta) = 0$ and $v_{\mathfrak{p}}(b) = 0$. Then we have:

$$f_{k(E_4)/k}(\mathfrak{p}) = \begin{cases} 1, \ if \ q \equiv 1 \ \mathrm{mod} \ 4, \ a_q \equiv 2 \ \mathrm{mod} \ 4, \\ \left(\frac{\Delta}{\mathfrak{p}}\right)_4 = 1 \ and \ B(X) \ has \ type \ (1, 1, 1, 1), \\ 2, \ if \ q \equiv 1 \ \mathrm{mod} \ 4, \ a_q \equiv 2 \ \mathrm{mod} \ 4, \\ \left(\frac{\Delta}{\mathfrak{p}}\right)_4 = -1 \ or \ B(X) \ has \ type \ (2, 2), \\ or \ q \equiv 3 \ \mathrm{mod} \ 4, \ a_q \equiv 0 \ \mathrm{mod} \ 4, \\ 3, \ if \ q \equiv 1 \ \mathrm{mod} \ 4, \ a_q \equiv 3 \ \mathrm{mod} \ 4, \ \left(\frac{\Delta}{\mathfrak{p}}\right)_4 = 1, \\ 4, \ if \ q \equiv 1 \ \mathrm{mod} \ 4, \ a_q \equiv 0 \ \mathrm{mod} \ 2, \ \left(\frac{\Delta}{\mathfrak{p}}\right)_4 \neq \pm 1, \\ or \ q \equiv 3 \ \mathrm{mod} \ 4, \ a_q \equiv 2 \ \mathrm{mod} \ 4, \ \left(\frac{\Delta}{\mathfrak{p}}\right)_2 = -1, \\ 6, \ if \ q \equiv 1 \ \mathrm{mod} \ 4, \ a_q \equiv 1 \ \mathrm{mod} \ 4, \ \left(\frac{\Delta}{\mathfrak{p}}\right)_4 = -1, \\ or \ q \equiv 3 \ \mathrm{mod} \ 4, \ a_q \equiv 1 \ \mathrm{mod} \ 4, \ \left(\frac{\Delta}{\mathfrak{p}}\right)_4 = -1, \\ or \ q \equiv 3 \ \mathrm{mod} \ 4, \ a_q \equiv 1 \ \mathrm{mod} \ 4, \ \left(\frac{\Delta}{\mathfrak{p}}\right)_4 = -1, \\ or \ q \equiv 3 \ \mathrm{mod} \ 4, \ a_q \equiv 1 \ \mathrm{mod} \ 2, \ \left(\frac{\Delta}{\mathfrak{p}}\right)_4 = -1, \\ or \ q \equiv 3 \ \mathrm{mod} \ 4, \ a_q \equiv 1 \ \mathrm{mod} \ 2, \ \left(\frac{\Delta}{\mathfrak{p}}\right)_4 = 1. \end{cases}$$

Proof.

We combine the results from Proposition 5.5.2 into one formula. The list of separate cases is derived from the conjugacy classes of GL(2, 4) as given in the leftmost column of Table 5.4. In order to distinguish between the classes, we must in some cases apply Theorem 2.1.1 and use the decomposition type of B(X). The classification is exhaustive since $LF = k(E_4)$. The complete description of all cases is given in Table 5.4.

83

Element	Necessary Conditions for			Type in	Order in			
of C	$\left(\frac{\mathbb{Q}(E_4)/\mathbb{Q}}{p}\right) \in C$			L	$\mathbb{Q}(\mu_4)$	$\mathbb{Q}(\mu_4,\sqrt[4]{\Delta})$	$\mathbb{Q}(E_2)$	$\mathbb{Q}(E_4)$
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$p \equiv 1 (4)$	$\Delta^{\frac{p-1}{4}} \equiv 1(p)$	$a_{p}\equiv2\left(4\right)$	(1,1,1,1)	1	1	1	1
$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$p \equiv 1 (4)$	$\Delta^{\frac{p-1}{4}} \equiv -1(p)$	$a_p \equiv 2 (4)$	(1,1,1,1)	1	2	1	2
$\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}$	$p \equiv 3 (4)$	$\Delta^{\frac{p-1}{2}} \equiv 1(p)$	$a_{p}\equiv0(4)$	(1,1,1,1)	2	2	1	2
$\begin{pmatrix} 1 & 2\\ 2 & 1 \end{pmatrix}$	$p \equiv 1 (4)$	$\Delta^{\frac{p-1}{4}} \equiv 1(p)$	$a_p \equiv 2 (4)$	(2,2)	1	1	1	2
$\begin{pmatrix} -1 & 2\\ 2 & -1 \end{pmatrix}$	$p \equiv 1 (4)$	$\Delta^{\frac{p-1}{4}} \equiv -1(p)$	$a_p \equiv 2 (4)$	(2,2)	1	2	1	2
$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$p \equiv 3 (4)$	$\Delta^{\frac{p-1}{2}} \equiv 1(p)$	$a_p \equiv 0 (4)$	(2,2)	2	2	1	2
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$p \equiv 3 (4)$	$\Delta^{\frac{p-1}{2}} \equiv -1(p)$	$a_{p}\equiv0(4)$	(2,1,1)	2	2	2	2
$\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$	$p \equiv 3(4)$	$\Delta^{\frac{p-1}{2}} \equiv -1(p)$	$a_p \equiv 2 (4)$	(4)	2	2	2	4
$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$p \equiv 1 (4)$	$\Delta^{\frac{p-1}{4}} \not\equiv \pm 1(p)$	$a_{p}\equiv0(4)$	(2,1,1)	1	4	2	4
$\begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}$	$p \equiv 1 (4)$	$\Delta^{\frac{p-1}{4}} \not\equiv \pm 1(p)$	$a_p \equiv 2 (4)$	(4)	1	4	2	4
$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$	$p \equiv 1 (4)$	$\Delta^{\frac{p-1}{4}} \equiv 1(p)$	$a_p \equiv 3(4)$	(3,1)	1	1	3	3
$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	$p \equiv 3(4)$	$\Delta^{\frac{p-1}{2}} \equiv 1(p)$	$a_p \equiv 1 (4)$	(3,1)	2	2	3	6
$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$	$p \equiv 3(4)$	$\Delta^{\frac{p-1}{2}} \equiv 1(p)$	$a_p \equiv 3 (4)$	(3,1)	2	2	3	6
$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$	$p \equiv 1 (4)$	$\Delta^{\frac{p-1}{4}} \equiv -1(p)$	$a_p \equiv 1 (4)$	(3,1)	1	2	3	6

Table 5.4. Decomposition in $\mathbb{Q}(E_4)/\mathbb{Q}$

We now again consider the base field $k = \mathbb{Q}$, E being defined over \mathbb{Q} . In Table 5.4 we describe the prime decomposition for all 14 conjugacy classes C of GL(2, 4). We assign to any class C a representative in the respective row, and we state the criteria of Proposition 5.5.2 as necessary conditions for a Frobenius automorphism to be a member of C. Moreover, for each class we give the decomposition type of the defining polynomial B(X) of the extension L/\mathbb{Q} which appears modulo a prime number p whose Frobenius automorphism belongs to the respective class. This condition can only be checked for unramified prime numbers p which are no divisors of the discriminant of B(X). The decomposition type of B(X) can be calculated most easily by determining the permutation corresponding to the considered class C under the isomorphism $\operatorname{GL}(2,4)/V_4 \cong \mathfrak{S}_4$ and then reading off its cycle type (as defined in Section 6.3).

We may see from Table 5.4 that the necessary conditions stated above are not sufficient to distinguish between the rows 1 and 4, 2 und 5, or 3 und 6, respectively. However, in order to know the decomposition law it is enough to know the orders of the respective Frobenius automorphisms. But even if we weaken our requirements appropriately, we still have to distinguish between the rows 1 and 4 so that we must additionally compute the decomposition type of the polynomial B(X) modulo the considered prime number p in order to finally obtain the decomposition law. The polynomial B(X) is only required to decide whether an unramified prime number $p \equiv 1 \mod 4$ satisfying the conditions $\Delta^{\frac{p-1}{4}} \equiv 1 \mod p$ and $a_p \equiv 2 \mod 4$ is fully decomposed in the extension $\mathbb{Q}(E_4)/\mathbb{Q}$ or whether it has inertial degree 2.

The classification in Table 5.4 can easily be generalized to number fields k. We only have to replace the prime number p by the prime ideal \mathfrak{p} of k with the norm q. The congruences of the second column will become conditions on q, those of the fourth column will change to conditions on a_q , and in the third column we have to replace the congruence by an appropriate condition on a corresponding power residue symbol.

5.6 Decomposition in p^m -Torsion Point Fields

We now summarize the results of the preceding sections. We have considered the extensions $k(E_n)/k$ of a number field k, where E is an elliptic curve over k with discriminant Δ , and we have assumed $\operatorname{Gal}(k(E_n)/k) \cong \operatorname{GL}(2, n)$.

Let \mathfrak{p} be a prime ideal in k with the absolute norm q. We require (q, n) = 1and $v_{\mathfrak{p}}(\Delta) = 0$, thus we ensure that \mathfrak{p} is unramified. When we want to describe the decomposition of \mathfrak{p} in $k(E_n)$, the following quantities are available:

- 1. We may use the order of q in $(\mathbb{Z}/n\mathbb{Z})^*$ because of $k(\mu_n) \subset k(E_n)$.
- 2. We may use the value of a_q modulo n, since a_q is the trace of the Frobenius element of \mathfrak{p} under the representation $\operatorname{Gal}(k(E_n)/k) \to \operatorname{GL}(2, n)$.
- 3. We may use defining polynomials of the respective subextensions.

We have reduced the general situation to the special case that the order n is the power of a prime number (see Proposition 5.2.1). These extensions can be written as composites of certain subfields in the following way.

Proposition 5.6.1.

(a) If p is an odd prime number, we have

$$\begin{split} k(E_{p^m}) &= k(\mu_{p^m}) \, k(J_{p^m}) \, k(E_p) \quad for \ m \geq 2, \\ k(x(E_p)) &= k(\mu_p) \, k(J_p). \end{split}$$

(b) Using the notation $k_{\Delta,4} = k(\mu_4, \sqrt[4]{\Delta})$, we have

$$\begin{aligned} k(E_2) &= k(J_2), \\ k(E_4) &= k(J_4) \, k_{\Delta,4}, \\ k(E_{2^m}) &= k(J_{2^m}) \, M_{2^m} \, k_{\Delta,4} \quad for \ m \geq 3, \end{aligned}$$

where M_{2m} corresponds to the fixed group $\pm W_{2m}$ as defined in (5.4), $k(\mu_{2m}, x(E_{2m-1}))$ being a subfield of index 2 in M_{2m} .

Proof.

We use Proposition 5.2.5 and apply induction on m.

85

Some important subextensions are defined by the following polynomials:

- $-k(\mu_n)/k$ is defined by the *n*-th cyclotomic polynomial $\phi_n(X)$,
- $-k(J_n)/k$ is defined by the *n*-th modular polynomial $\Phi_n(X, j(E))$,
- M_{2^m}/k is defined by some polynomial $Q_{2^m}(X)$.

The subfields mentioned in Proposition 5.6.1 are in general not linearly disjoint. Thus there are some inherent dependencies between the quantities of the above list. Our result is as follows:

Proposition 5.6.2.

The decomposition of \mathfrak{p} in $k(E_{p^m})$ is uniquely determined if all of the following quantities are known.

- 1. The order of $q \mod p^m$ in $(\mathbb{Z}/p^m\mathbb{Z})^*$,
- 2. The decomposition type of $\Phi_{p^m}(X, j(E))$ in $\mathbb{F}_q[X]$,
- 3. For $p \neq 2$, the value of a_q modulo p,

4. For
$$p = 2$$
, $m \ge 2$, the order of $\begin{cases} \left(\frac{\Delta}{\mathfrak{p}}\right)_4, & \text{if } q \equiv 1 \mod 4, \\ \left(\frac{\Delta}{\mathfrak{p}}\right)_2, & \text{if } q \equiv 3 \mod 4, \end{cases}$

5. For p = 2, $m \ge 3$, the decomposition type of $Q_{2^m}(X)$ in $\mathbb{F}_q[X]$.

Proof.

This is the result of the previous sections. In particular, we refer to Corollary 2.2.1, Proposition 5.5.2 and Proposition 5.6.1. □

We separately state necessary and sufficient conditions on the prime ideal \mathfrak{p} of k to be fully decomposed in $k(E_{p^m})/k$.

Proposition 5.6.3.

The prime ideal \mathfrak{p} with the norm q is fully decomposed in $k(E_{p^m})/k$ if and only if each of the following conditions is satisfied.

- 1. $q \equiv 1 \mod p^m$, 2. $\Phi_{p^m}(X, j(E))$ splits in $\mathbb{F}_q[X]$ into distinct linear factors, 3. $a_q \equiv 2 \mod p$,
- 4. for p = 2, $m \ge 2$, we have $\left(\frac{\Delta}{\mathfrak{p}}\right)_4 = 1$,
- 5. for $p = 2, m \ge 3, Q_{2^m}(X)$ splits in $\mathbb{F}_{q}[X]$ into distinct linear factors.

If the quantities a_q resulted from a representation over a field of characteristic 0, they would uniquely determine the decomposition behaviour of \mathfrak{p} , but this is not the case. In fact, if $n = p^m$ is a prime power, we cannot distinguish between the elements of $D_{p^m} = \mathrm{SL}(2, p^m) \cap R_{p^m}$, and if n = p is a prime number, we cannot distinguish $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ from $\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$.

Most difficulties in our investigations appear in the extensions $k(E_p)/k$ for prime numbers $p \ge 5$ because the subextensions $k(J_p)/k(\sqrt{p^*})$ are simple, that is, they have no Galois intermediate fields.

6 Invariants and Resolvent Polynomials

In Section 5.5 we encountered the problem of describing a subfield of a given Galois extension K/k of algebraic number fields. This problem can be dealt with independently from the other results achieved so far. The geometric information gained may be seen as a tool to uniquely determine the shape of the Galois group and to give initial data and conditions to the coefficients of those polynomials which are used to perform the following characterization of the given subfield.

We review some facts of Galois theory in Section 6.1 to fix our notations.

Section 6.2 describes the method of calculating an appropriate polynomial by interpreting the Galois group of the field extension as symmetry group or permutation group of the zeroes of the wanted polynomial.

The strategy of solving the above problem is in close connection to invariant algebras over k whose properties are listed in Section 6.3.

In Section 6.4 we apply the indicated procedure to the subfield L, which we have encountered in the previous chapter. L is a subfield of the extension $k(x(E_4))/k$ of an algebraic number field k generated by the x-coordinates of all 4-torsion points of an elliptic curve E. The result we achieve below has already been applied in Section 5.5.

6.1 Foundations of Galois Theory

Given a field k and a polynomial $f(Y) \in k[Y]$ of degree $m \ge 1$, we let

$$N_f = \{ \alpha \in \hat{k} \mid f(\alpha) = 0 \}$$

denote the set of zeroes of f contained in some fixed algebraic closure \hat{k} of k. By adjoining all zeroes of N_f to k we get an extension field k_f of k which is uniquely defined as a subfield of \hat{k} . k_f is called the *splitting field* of the polynomial f. k_f is the intersection of all extension fields K of k contained in \hat{k} such that f(Y) splits into linear factors in the polynomial ring K[Y].

In order to work with the zeroes of f(Y), we initially fix a particular order of the zeroes, that is, we define a surjective enumeration map

$$\nu : \{1, \dots, m\} \to N_f , \\ i \mapsto \alpha_i$$

C. Adelmann: LNM 1761, pp. 87–106, 2001.

[©] Springer-Verlag Berlin Heidelberg 2001

such that we have $f(Y) = \prod_{i=1}^{m} (Y - \alpha_i)$ in $\hat{k}[Y]$.

Any possible enumeration map has the shape $\nu \circ \pi$ for some $\pi \in \mathfrak{S}_m$.

Since the zeroes are generally not known, they are to be treated like indeterminates. We consider therefore the polynomial algebra $k[x_1, \ldots, x_m]$ in *m* algebraically independent indeterminates. Each permutation $\pi \in \mathfrak{S}_m$ induces a *k*-algebra automorphism $\overline{\pi}$ of $k[x_1, \ldots, x_m]$ by the rule $x_i \mapsto x_{\pi(i)}$ which is for $P \in k[x_1, \ldots, x_m]$ explicitly given by $P \mapsto \overline{\pi}(P)$ satisfying

$$\overline{\pi}(P)(x_1,\ldots,x_m) = P(x_{\pi(1)},\ldots,x_{\pi(m)}).$$
(6.1)

In this way, $\overline{\mathfrak{S}}_m = \{ \overline{\pi} \mid \pi \in \mathfrak{S}_m \}$ is a subgroup of $\operatorname{Aut}_k(k[x_1, \ldots, x_m])$ which is isomorphic to \mathfrak{S}_m .

Let U be a subgroup of $\overline{\mathfrak{S}}_m$. To any polynomial $P \in k[x_1, \ldots, x_m]$ we assign its stabilizer subgroup

$$\operatorname{Stab}_U(P) = \{ \, \overline{\pi} \in U \mid \overline{\pi}(P) = P \, \} \, .$$

The polynomial $P \in k[x_1, \ldots, x_m]$ is called *U*-invariant if it remains fixed under the operation of all elements of U, i. e. if we have $U \leq \operatorname{Stab}_{\overline{\mathfrak{S}}_m}(P)$.

The set of all U-invariant polynomials (U-invariants for short) lying in $k[x_1, \ldots, x_m]$ forms a k-subalgebra which is denoted by $k[x_1, \ldots, x_m]^U$. The map $U \mapsto k[x_1, \ldots, x_m]^U$ is inclusion reversing. In particular, the subalgebra $k[x_1, \ldots, x_m]^{\mathfrak{S}_m}$ of symmetric polynomials is contained in all invariant algebras, that is in all algebras of the shape $k[x_1, \ldots, x_m]^U$.

Let $\omega_{f,\nu} = \omega_f : k[x_1, \ldots, x_m] \to k_f$ denote the surjective evaluation homomorphism given by $x_i \mapsto \alpha_i$ and depending on the enumeration map ν . Its kernel is the ideal

$$R_f = \ker(\omega_f) = \{ P \in k[x_1, \dots, x_m] \mid P(\alpha_1, \dots, \alpha_m) = 0 \},\$$

the set of all k-polynomial relations between the zeroes of f. In this situation, a given permutation of the zeroes of f is an element of the Galois group of the polynomial f over k if and only if none of the k-polynomial relations becomes invalid,

$$\operatorname{Gal}(f/k) = \{ \pi \in \mathfrak{S}_m \mid \overline{\pi}(R_f) \subseteq R_f \}.$$
(6.2)

In order to establish a bijective correspondence between the Galois group of a polynomial and the automorphism group of its splitting field, we have to restrict our attention to

- Separable polynomials f whose derivatives do not vanish identically,
- Polynomials f without multiple zeroes,
- Separable field extensions K/k.

On these assumptions we get $|N_f| = m$, and the splitting field k_f is a normal, separable extension. Its group of k-automorphisms $\operatorname{Aut}_k(k_f)$ is called the Galois group $\operatorname{Gal}(k_f/k)$ of the extension k_f/k . Since k_f is generated by N_f over k, $\operatorname{Gal}(k_f/k)$ operates faithfully on N_f .

If we define the permutation belonging to $\sigma \in \text{Gal}(k_f/k)$ by the rule $\pi_{\sigma} = \nu^{-1} \circ \sigma|_{N_f} \circ \nu$, we get an injective group homomorphism

$$r_{\nu} : \operatorname{Gal}(k_f/k) \to \mathfrak{S}_m .$$

 $\sigma \mapsto \pi_{\sigma}$

For all $\sigma \in \text{Gal}(K/k)$ we have a commutative diagram of k-algebras

$$k[x_1, \dots, x_m] \xrightarrow{\pi_{\sigma}} k[x_1, \dots, x_m]$$

$$\downarrow \omega_f \qquad \qquad \downarrow \omega_f$$

$$k_f \xrightarrow{\sigma} \qquad k_f$$

We notice the property $\alpha_{\pi_{\sigma}(i)} = \sigma(\alpha_i)$.

Proposition 6.1.1.

- (a) Let $H \leq \text{Gal}(k_f/k)$, such that the characteristic of k is no divisor of |H|. Then we have $\omega_f(k[x_1, \dots, x_m]^{r_\nu(H)}) = k_f^H$.
- (b) We have the equality $\operatorname{Gal}(f/k) = r_{\nu}(\operatorname{Gal}(k_f/k)).$

Proof.

(a) For $\sigma \in H$ and $P \in k[x_1, \ldots, x_m]^{r_{\nu}(H)}$, we have

$$\omega_f(P) = \omega_f \circ \overline{\pi_\sigma}(P) = \sigma \circ \omega_f(P), \quad \text{hence} \quad \omega_f(P) \in k_f^H.$$

Conversely, if $a \in k_f^H$ then, because of $k_f = k[\alpha_1, \ldots, \alpha_m]$, there is some $P \in k[x_1, \ldots, x_m]$ satisfying $\omega_f(P) = a$. If we set $Q = \frac{1}{|H|} \sum_{\tau \in H} \overline{\pi_\tau}(P)$, we have $Q \in k[x_1, \ldots, x_m]^{r_\nu(H)}$ and $\omega_f(Q) = a$.

(b) For $\sigma \in \text{Gal}(k_f/k)$ and $P \in R_f$, we have

$$\omega_f \circ \overline{\pi_\sigma}(P) = \sigma \circ \omega_f(P) = \sigma(0) = 0$$
, whence $\overline{\pi_\sigma}(P) \in R_f$.

Conversely, if $\pi \in \text{Gal}(f/k)$ then, because of $\overline{\pi}(R_f) \subseteq R_f$, $\overline{\pi}$ defines a k-automorphism σ_{π} of $k[x_1, \ldots, x_m]/R_f \cong k_f$. We conclude

$$\alpha_{\pi(i)} = \omega_f \circ \overline{\pi}(x_i) = \sigma_{\pi} \circ \omega_f(x_i) = \sigma_{\pi}(\alpha_i), \quad \text{hence} \quad \pi_{\sigma_{\pi}} = \pi. \qquad \Box$$

By Proposition 6.1.1 the Galois group of a polynomial and the Galois group of its splitting field are isomorphic.

For $\pi \in \mathfrak{S}_m$ we have $r_{\nu \circ \pi}(\operatorname{Gal}(k_f/k)) = \pi^{-1} r_{\nu}(\operatorname{Gal}(k_f/k)) \pi$, i. e. the images of $\operatorname{Gal}(k_f/k)$ with respect to different enumeration maps are conjugate in \mathfrak{S}_m . In particular, $\operatorname{Gal}(f/k)$ is determined up to conjugation as a subgroup of \mathfrak{S}_m .

The order of the zeroes $\{\alpha_1, \ldots, \alpha_m\}$ of f(Y) given by the enumeration map ν is considered fixed in the following sections.

6.2 Procedure for the Description of Subfields

Let k be an algebraic number field and \overline{k} a fixed separable closure of k. The following data may be given:

- A Galois extension K/k and a defining polynomial A(Y) of K over k,

$$A(Y) = a_m Y^m + a_{m-1} Y^{m-1} + \ldots + a_1 Y + a_0 \quad \text{with} \quad a_i \in k \ , \ a_m \neq 0,$$

i. e. an irreducible polynomial whose splitting field is equal to K in \overline{k} ,

- A realization of $\operatorname{Gal}(K/k)$ as subgroup of \mathfrak{S}_m , i. e. an injective group homomorphism $r: \operatorname{Gal}(K/k) \to \mathfrak{S}_m$.
- A subgroup H of $\operatorname{Gal}(K/k)$.

We are looking for a description of the fixed field K^H belonging to H, for instance by giving a defining polynomial of K^H over k of the kind

$$B(Y) = b_t Y^t + b_{t-1} Y^{t-1} + \ldots + b_1 Y + b_0, \quad \text{with} \quad b_i \in k, \ b_t \neq 0.$$

In a general situation, B(Y) is the minimal polynomial of some primitive element of K^H , i. e. K^H is constructed from k by adjoining exactly one zero of B(Y). However, if H is a normal subgroup, it may be useful to look for some polynomial B(Y) whose splitting field is equal to K^H , so that K^H is constructed by adjoining all zeroes of B(Y). In many cases, the degree of such a polynomial is much smaller than the degree of the minimal polynomial of any primitive element. In order to pursue this aim, we have to find a subgroup \tilde{H} of $\operatorname{Gal}(K/k)$ satisfying $H \subseteq \tilde{H}$ and which is as large as possible, such that the intersection of all conjugates of \tilde{H} in $\operatorname{Gal}(K/k)$ is equal to H. We can then apply the procedure given below to \tilde{H} instead of H.

The procedure sought for should express the coefficients b_j in a most efficient way as polynomials or rational functions in the a_i with coefficients from k. During the process, any operation should only be performed to quantities which are taken from the base field.

The problem stated above to calculate defining polynomials can be solved with the aid of the invariant algebras $k[x_1, \ldots, x_m]^U$, where we return to the notation of Section 6.1. In order to do this, we have to be able to gain the following data in a most effective way for any subgroup U of $\overline{\mathfrak{S}}_m$:

- A set of generators of $k[x_1, \ldots, x_m]^U$ over k as a k-algebra,
- The representation of any element of $k[x_1, \ldots, x_m]^U$ as a polynomial in these generators,
- The image of each element of the generating set under ω_f .

If H is the given subgroup of $\operatorname{Gal}(K/k)$ and $G = r(\operatorname{Gal}(K/k))$, we search for a polynomial P of $k[x_1, \ldots, x_m]$ which remains invariant with respect to G exactly under the operation of the permutations from r(H) i. e. which satisfies $\operatorname{Stab}_G(P) = r(H)$. We hope that such an invariant P is mapped

by ω_f to a primitive element of the fixed field K^H . In this case the corresponding minimal polynomial in k[Y] is the image of a polynomial from $k[x_1,\ldots,x_m][Y]$ under ω_f whose coefficients can be expressed by the generators of $k[x_1, \ldots, x_m]^{\overline{G}}$, so that substituting the images of the generators provides a formula for the coefficients of the polynomial to be determined.

In the following section, we state this idea more precisely and we explain under which conditions this strategy is successful. For this purpose we need some basic facts on the invariant algebras $k[x_1, \ldots, x_m]^U$.

6.3 Invariant Algebras

In this section we list some important properties of invariant algebras. The description is oriented to [Stu93, Chap. 2], see also [Bens93, Chap. 1, Chap. 2].

Let A be a graded k-algebra, i. e. A has a decomposition $A = \bigoplus_{d>0} A_d$ with $A_0 = k$ and $A_i \cdot A_i \subseteq A_{i+i}$ where A_d is called the homogenous component of A of degree d. If all homogenous components are finite dimensional k-vector spaces, we define the *Hilbert-series* (or Poincaré-series) Φ_A of A as generating function with coefficients equal to the respective dimensions,

$$\Phi_A(z) = \sum_{d \ge 0} \dim_k(A_d) \, z^d \, .$$

The Krull dimension of a graded ring A is the maximal length of a chain of prime ideals of A properly contained in one another. If we consider a graded k-algebra, its Krull dimension coincides with the maximal number of elements which are algebraically independent over k.

If A is a graded k-algebra of Krull dimension m then, by the Noether normalization lemma (see [Stu93, 2.3, p. 37]), there are m homogenous elements $\theta_1, \ldots, \theta_m$ of strictly positive degree so that A is a finitely generated module over $k[\theta_1, \ldots, \theta_m]$. Such a set $\{\theta_1, \ldots, \theta_m\}$ is called a *homogenous set* of parameters of A.

If in addition A is a free module over $k[\theta_1, \ldots, \theta_m]$ then this property holds for all homogenous sets of parameters of A (see [Stu93, Thm. 2.3.1]). In this case the graded algebra A is called a Cohen-Macaulay algebra. Any Cohen-Macaulay algebra A of Krull dimension m therefore possesses a decomposition

$$A = \bigoplus_{i=1}^{t} \eta_i \ k[\theta_1, \dots, \theta_m]$$
(6.3)

in which $\theta_1, \ldots, \theta_m$ are homogenous and algebraically independent and $\{\eta_1, \ldots, \eta_t\}$ forms a homogenous module basis of A over $k[\theta_1, \ldots, \theta_m]$. A decomposition of the shape (6.3) is called *Hironaka decomposition* of A. It is not unique in general, even the degrees of the generators are not uniquely determined. At least, we are able to deduce the Hilbert-series of A from a Hironaka decomposition of A.

Proposition 6.3.1.

Let the graded algebra A be a Cohen-Macaulay algebra of Krull dimension m which possesses a Hironaka decomposition of the form (6.3). Then the Hilbertseries of A is

$$\Phi_A(z) = \frac{z^{\deg \eta_1} + \ldots + z^{\deg \eta_t}}{(1 - z^{\deg \theta_1}) \cdot \ldots \cdot (1 - z^{\deg \theta_m})} .$$

Proof. See [Stu93, Cor. 2.3.4].

However, there are non-isomorphic graded k-algebras having identical Hilbertseries (see e. g. [Smi95, 4 § 1 Ex. 1, p. 77]).

Now let U be a subgroup of \mathfrak{S}_m . The first problem in connection with invariants is to gain elements from $k[x_1, \ldots, x_m]^U$. To solve it, we use the following constructions.

1. The averaging operator or Reynolds operator R_U of U,

$$R_U : k[x_1, \dots, x_m] \to k[x_1, \dots, x_m]^U ,$$

$$P \qquad \mapsto \frac{1}{|U|} \sum_{\pi \in U} \pi(P)$$

calculates (up to a scalar factor) the trace of the operation of U on $k[x_1, \ldots, x_m]$.

2. The formal resolvent polynomial is for subgroups $W \leq U \leq \mathfrak{S}_m$ and W-invariants $P \in k[x_1, \ldots, x_m]^W$ given by

$$\mathcal{RP}_{W \le U}(P)(Y) = \prod_{\pi \in U/W} (Y - \pi(P)) , \qquad (6.4)$$

where π runs through the left cosets of W in U. If $W = \operatorname{Stab}_U(P)$, we write $\mathcal{RP}_U(P)$ instead of $\mathcal{RP}_{W \leq U}(P)$.

The proposition below states the basic linearity and homomorphy properties of the Reynolds operator.

Proposition 6.3.2.

(a) R_U is k-linear and equal to the identity on $k[x_1, \ldots, x_m]^U$. We get the decomposition

$$k[x_1,\ldots,x_m] = k[x_1,\ldots,x_m]^U \oplus \ker(R_U).$$

(b) R_U is a homomorphism of $k[x_1, \ldots, x_m]^U$ -modules, i. e.

$$R_U(f \cdot g) = R_U(f) \cdot g \quad \text{for} \quad f \in k[x_1, \dots, x_m], \ g \in k[x_1, \dots, x_m]^U$$

Proof.

The result may be concluded from [Stu93, Prop. 2.1.2].

In the form given above, the Reynolds operator is a projection mapping by Proposition 6.3.2 (a). However, fractional scalar factors appear which do not cause any real difficulty since the base field has characteristic 0 but which may lead to unwieldy results and which can easily be avoided. For $P \in k[x_1, \ldots, x_m]$ and $W = \operatorname{Stab}_U(P)$ we modify the Reynolds operator by

$$\overline{R}_U(P) = \sum_{\pi \in U/W} \pi(P) \; ,$$

where π runs through the left cosets of W in U.

The importance of the formal resolvent polynomial is founded on the invariance property of its coefficients which is the result of the following proposition.

Proposition 6.3.3.

For $P \in k[x_1, \ldots, x_m]^W$ we have $\mathcal{RP}_{W \leq U}(P)(Y) \in (k[x_1, \ldots, x_m]^U)[Y]$.

Proof.

Any $\pi \in U$ induces a permutation of the cosets of W in U and therefore of the linear factors of $\mathcal{RP}_{W \leq U}(P)(Y)$ in (6.4), so that their product remains invariant under π . In particular, the coefficients of the formal resolvent polynomial are U-invariant.

Remark 6.3.1.

The Reynolds operator appears as a coefficient of a certain formal resolvent polynomial: Let $P \in k[x_1, \ldots, x_m]$ and $W = \operatorname{Stab}_U(P)$. Then the second coefficient, i. e. the coefficient of $Y^{(U:W)-1}$ in $\mathcal{RP}_U(P)(Y)$ is equal to $-\overline{R}_U(P)$ or equal to $-(U:W) \cdot R_U(P)$, respectively.

If a set of generators for the ring of invariants $k[x_1, \ldots, x_m]^U$ is known, we can express by Proposition 6.3.3 the coefficients of the formal resolvent polynomial $\mathcal{RP}_{W \leq U}(P)$ in terms of polynomials in the generators.

The next proposition asserts that the quotient field of the ring of invariants $k[x_1, \ldots, x_m]^U$ has transcendence degree m over k.

Proposition 6.3.4.

There are m algebraically independent elements in $k[x_1, \ldots, x_m]^U$. The Krull dimension of $k[x_1, \ldots, x_m]^U$ over k is equal to m.

Proof. ([Stu93, Prop. 2.1.1])

 $P_i(x_1, \ldots, x_m, Y) = \mathcal{RP}_U(x_i)(Y)$ is a polynomial from $(k[x_1, \ldots, x_m]^U)[Y]$ with the zero $Y = x_i$. The elements x_1, \ldots, x_m are therefore algebraically dependent from certain appropriate U-invariants so that at least m algebraically independent U-invariants have to exist. There cannot be more than m because of $k[x_1, \ldots, x_m]^U \subseteq k[x_1, \ldots, x_m]$.

Proposition 6.3.5.

The algebra $k[x_1, \ldots, x_m]^U$ of U-invariants is a Cohen-Macaulay algebra.

Proof.

See [Stu93, Thm. 2.3.5].

Consequently, $k[x_1, \ldots, x_m]^U$ has a Hironaka decomposition (6.3). The set of generators $\{\theta_1, \ldots, \theta_m, \eta_1, \ldots, \eta_t\}$ is called a set of *fundamental invariants* of U. The θ_i are named *primary invariants*, the η_j are named *secondary invariants*.

Theorem 6.3.1. (Noether)

The algebra $k[x_1,\ldots,x_m]^U$ is generated over k by the set

$$\{ R_U(x_1^{e_1} \cdot \ldots \cdot x_m^{e_m}) \mid e_i \ge 0, e_1 + \ldots + e_m \le |U| \}.$$

Therefore $k[x_1, \ldots, x_m]^U$ has a k-algebra basis with at most $\binom{m+|U|}{m}$ elements with degrees $\leq |U|$.

Proof. See [Stu93, Thm. 2.1.4].

Thinking of $k[x_1, \ldots, x_m]$ as a *m*-dimensional *k*-vector space, every algebra automorphism of $k[x_1, \ldots, x_m]$ can be written as an $m \times m$ -matrix. In this way, any permutation $\pi \in \mathfrak{S}_m$ is assigned to a permutation matrix $M(\pi)$ with entries equal to 0 or 1.

Theorem 6.3.2. (Molien)

The Hilbert-series Φ_U of $k[x_1, \ldots, x_m]^U$ is given by

$$\Phi_U(z) = \frac{1}{|U|} \sum_{\pi \in U} \frac{1}{\det(\mathbf{1} - z \cdot M(\pi))}$$

Proof. See [Stu93, Thm. 2.2.1].

The number of primary invariants is equal to the Krull dimension of the algebra $k[x_1, \ldots, x_m]^U$ and is therefore equal to m. The number t of secondary invariants is in general not uniquely determined. If a set of primary invariants $\{\theta_1, \ldots, \theta_m\}$, however, is already given, we can deduce the value of t from their degrees by means of Theorem 6.3.2.

Proposition 6.3.6.

The number t of secondary invariants satisfies $t = \frac{\deg \theta_1 \cdot \ldots \cdot \deg \theta_m}{|U|}$.

Proof.

See [Stu93, Prop. 2.3.6]. We calculate $\lim_{z\to 1} (1-z)^m \Phi_U(z)$.

The permutation $\pi \in \mathfrak{S}_m$ is said to have the *cycle type* (ℓ_1, \ldots, ℓ_r) for integers $\ell_i \geq 1$ with $\ell_1 + \ldots + \ell_r = m$ if π is a product of exactly r cipher disjoint cycles of respective lengths ℓ_1, \ldots, ℓ_r . Any π possesses a uniquely determined cycle type if we additionally require $\ell_1 \geq \ldots \geq \ell_r$.

If U is known as a subgroup of \mathfrak{S}_m , we can calculate the summands of the Hilbert-series in terms of the cycle types of the permutations in U, for we have the following proposition.

Proposition 6.3.7.

Let $\pi \in \mathfrak{S}_m$ be a permutation with cycle type (ℓ_1, \ldots, ℓ_r) . Then it holds

$$\det(\mathbf{1} - z \cdot M(\pi)) = \prod_{i=1}^{r} (1 - z^{\ell_i}) \, .$$

Proof.

A product of cipher disjoint cycles corresponds under M to an automorphism of a direct sum of vector subspaces of $k[x_1, \ldots, x_m]$. A cycle of length ℓ_i has the minimal polynomial $1 - z^{\ell_i}$, and the characteristic polynomial of $M(\pi)$ is calculated as the product of the minimal polynomials of the cipher disjoint cycles in π (cf. [Stu93, 2.7.7]).

Now we take into account the operation of the Galois group $\operatorname{Gal}(K/k)$ to be examined. We extend the evaluation homomorphism ω_f by the trivial operation $Y \mapsto Y$ to give $\omega_f : k[x_1, \ldots, x_m][Y] \to K[Y]$ and define the resolvent polynomial $\mathcal{R}_{U,P}(Y) \in k[Y]$ belonging to $P \in k[x_1, \ldots, x_m]$ by

$$\mathcal{R}_{U,P}(Y) = \omega_f(\mathcal{RP}_U(P)(Y)) \; .$$

This notion is modelled on classical examples (compare it to the treatments in [Dehn60, §38,§66] or [Cohe93, Def. 6.3.2]). A resolvent in the sense of Lagrange or Galois is a zero of a particular resolvent polynomial by means of which a given equation is to be solved or simplified. The statement of the following proposition provides a crucial ingredient to coping with the initial problem to describe the unknown subextension of K/k.

Theorem 6.3.3.

Let $U \leq \mathfrak{S}_m$ with $G \leq U$. Let $P \in k[x_1, \ldots, x_m]$ be a polynomial, and set $W = \operatorname{Stab}_U(P)$. Let $\mathcal{R}_{U,P}(Y)$ be the resolvent polynomial belonging to P and

$$\mathcal{R}_{U,P}(Y) = \prod_{i=1}^{s} g_i^{a_i}(Y)$$

the decomposition of $\mathcal{R}_{U,P}(Y)$ into a product of powers of distinct irreducible polynomials in k[Y]. If $\operatorname{IrrP}(\mathcal{R}_{U,P}(Y), k)$ denotes the set $\{g_1^{a_1}(Y), \ldots, g_s^{a_s}(Y)\}$ then we have a bijection 96 6 Invariants and Resolvent Polynomials

$$G \setminus U/W \to IrrP(\mathcal{R}_{U,P}(Y), k)$$

$$G\pi W \mapsto g_{\pi}(Y) = \prod_{\tau W \subseteq G\pi W} \omega_f(Y - \tau(P))$$

The product for $g_{\pi}(Y)$ runs through the left cosets τW of W in U contained in $G\pi W$, i. e. through $\tau = \pi_{\sigma} \pi$ where π_{σ} runs through a system of representatives of the left cosets of $G \cap \pi W \pi^{-1}$ in G.

Proof.

(i) $g_{\pi}(Y) \in k[Y]$. For $\sigma \in \text{Gal}(K/k)$ we have

$$\sigma(g_{\pi}(Y)) = \prod_{\tau W \subseteq G\pi W} \omega_f(Y - \pi_{\sigma} \tau(P)).$$

Multiplication on the left by $\pi_{\sigma} \in G$ permutes the cosets of $G \cap \pi W \pi^{-1}$ in G and consequently the cosets τW contained in $G\pi W$, since we conclude from $\tau W \subseteq G\pi W$ that $\pi_{\sigma}\tau W \subseteq G\pi W$ holds for all $\pi_{\sigma} \in G$, and the equality $\pi_{\sigma}\pi W = \pi_{\sigma'}\pi W$ leads to $\pi_{\sigma}^{-1}\pi_{\sigma'} \in G \cap \pi W \pi^{-1}$. σ only causes a permutation of the factors in the product above, and we have $\sigma(g_{\pi}(Y)) = g_{\pi}(Y)$ for all $\sigma \in \text{Gal}(K/k)$.

- (ii) $g_{\pi}(Y)$ divides $\mathcal{R}_{U,P}(Y)$. Only a subset of the linear factors from which the resolvent polynomial is formed appears in the product expression of $g_{\pi}(Y)$ (see (6.4)).
- (iii) The zeroes of $g_{\pi}(Y)$ are conjugate under $\operatorname{Gal}(K/k)$. Given $\tau_1 W, \tau_2 W \subseteq G \pi W$, we find a $\pi_{\sigma} \in G$ satisfying $\pi_{\sigma} \tau_1 W = \tau_2 W$. Hence we conclude $\sigma(\omega_f(\tau_1(P))) = \omega_f(\tau_2(P))$ for some $\sigma \in \operatorname{Gal}(K/k)$.
- (iv) Conjugate zeroes of $\mathcal{R}_{U,P}(Y)$ correspond to the same double coset. Assume $\sigma(\omega_f(\pi_1(P))) = \omega_f(\pi_2(P))$ for $\sigma \in \operatorname{Gal}(K/k)$ and $\pi_1, \pi_2 \in U$. Then we have $\pi_2^{-1}\pi_\sigma\pi_1 \in W$, hence $\pi_\sigma\pi_1W = \pi_2W$ and $G\pi_1W = G\pi_2W$.
- (v) Any irreducible factor of $\mathcal{R}_{U,P}(Y)$ appears in one of the factors $g_{\pi}(Y)$. Any linear factor has the shape $\omega_f(Y - \pi(P))$ for some $\pi \in U$ and therefore divides $g_{\pi}(Y)$.

By (iii), $g_{\pi}(Y)$ is the power of a polynomial which is irreducible over k[Y], and by (iv), $g_{\pi}(Y)$ and $g_{\pi'}(Y)$ are coprime if $G\pi W$ and $G\pi' W$ are different cosets. Therefore the polynomial

$$F(Y) = \prod_{G\pi_i W \in G \setminus U/W} g_{\pi_i}(Y)$$

 $(\pi_i \text{ running through a system of representatives of the double cosets of <math>G \setminus U/W$) is a divisor of $\mathcal{R}_{U,P}(Y)$, i. e. using an appropriate numbering of the indices, we have $g_{\pi_i}(Y) = g_i^{b_i}(Y)$ with $0 < b_i \leq a_i$ for all *i*. The degree of $g_{\pi_i}(Y)$ is equal to the number of cosets of *W* contained in $G\pi_iW$, that is

$$\deg g_{\pi_i}(Y) = \frac{|G\pi_i W|}{|W|} = \frac{|G|}{|G \cap \pi_i W \pi_i^{-1}|}.$$

Since the double cosets of U form a partition of the set U, we have (cf. [Hupp67, I. 2.19])

$$\deg F(Y) = \sum_{i} \deg g_{\pi_{i}}(Y) = \sum_{i} \frac{|G|}{|G \cap \pi_{i} W \pi_{i}^{-1}|} = \frac{|U|}{|W|} = \deg \mathcal{R}_{U,P}(Y) ,$$

consequently we have $b_i = a_i$ for all *i*.

Remark 6.3.2.

Multiple factors do indeed appear in a resolvent polynomial if there is an interaction between P and R_f .

Let for example $k = \mathbb{Q}$ and K be the splitting field of $Y^4 + 1$. Then we have $G = \{(), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ as a subgroup of \mathfrak{S}_4 . If we choose $U = \mathfrak{A}_4$ and $P = x_1 x_2$, we get $\operatorname{Stab}_{\mathfrak{S}_4}(x_1 x_2) = \{(), (1, 2), (3, 4), (1, 2)(3, 4)\}$ and $W = \operatorname{Stab}_{\mathfrak{A}_4}(x_1 x_2) = \{(), (1, 2)(3, 4)\}$. The resolvent polynomial of $x_1 x_2$ with respect to \mathfrak{A}_4 is calculated as

$$\mathcal{R}_{\mathfrak{A}_4, x_1 x_2}(Y) = (Y+1)^2 (Y-1)^2 (Y^2+1).$$

A similar example can be found in [Dehn60, §64].

Proposition 6.3.8.

Let $U \leq \mathfrak{S}_m$ with $G \leq U$, let $P \in k[x_1, \ldots, x_m]$ be a polynomial with stabilizer $W = \operatorname{Stab}_U(P)$. G is conjugate to a subgroup of W if and only if the resolvent polynomial $\mathcal{R}_{U,P}(Y)$ possesses a non-repeated linear factor.

Proof.

 $1 = \deg g_{\pi}(P) = \frac{|G|}{|G \cap \pi W \pi^{-1}|} \text{ if and only if } G \text{ is a subgroup of } \pi W \pi^{-1}. \qquad \Box$

The resolvent polynomial is particularly suited to investigations of field extensions if it does not possess any multiple factor. This can always be guaranteed if we possibly apply a Tschirnhaus transformation to the defining polynomial A(Y) of the extension K/k (see [Cohe93, Alg. 6.3.4]). For that purpose we look for an appropriate polynomial $Q(Y) \in k[Y]$ of degree $\leq m-1$ and replace A(Y) by

$$\hat{A}(Y) = \operatorname{Res}_X(A(X), Y - Q(X)),$$

that is, we calculate the resultant of the mentioned polynomials with respect to the variable X, and then we still have to check to see that $\hat{A}(Y)$ does not contain any repeated factor.

If we finally reach the point that in our resolvent polynomial only simple factors appear, we can uniquely identify the Galois group of the corresponding splitting field which is a subfield of the Galois extension K/k.

Theorem 6.3.4.

Let $U \leq \mathfrak{S}_m$ with $G \leq U$, let $P \in k[x_1, \ldots, x_m]$ with stabilizer $W = \operatorname{Stab}_U(P)$ and let n = (U : W) be the index of W in U. Let us assume that the resolvent polynomial $\mathcal{R}_{U,P}(Y)$ has no multiple factor. Then we have:

- (a) For $\pi \in U$ the fixed group of the field $L = k(\omega_f(\pi(P)))$ corresponds to $G \cap \pi W \pi^{-1}$.
- (b) If M is the splitting field of $\mathcal{R}_{U,P}(Y)$ contained in K, the quotient group $\operatorname{Gal}(M/k)$ of $\operatorname{Gal}(K/k)$ corresponds to G/D with

$$D = G \cap \bigcap_{\pi \in U} \pi W \pi^{-1}$$

(c) If $\phi : U \to \mathfrak{S}_n$ denotes the permutation representation of U on the left cosets of U/W given by multiplication on the left by elements from U, we get a realization H of Gal(M/k) as a subgroup of \mathfrak{S}_n by letting $H = \phi(G)$.

Proof.

- (a) Any $\pi_{\sigma} \in G \cap \pi W \pi^{-1}$ corresponds to an automorphism $\sigma \in \text{Gal}(K/k)$ which fixes *L*. Conversely, if σ is such an automorphism, $\omega_f(\pi(P))$ is mapped to itself since $\mathcal{R}_{U,P}(Y)$ has no repeated factors. So we conclude $\pi_{\sigma} \in G \cap \pi W \pi^{-1}$.
- (b) M is the composite of all fields L of the shape given in (a) and consequently has a fixed group corresponding to the normal subgroup D of G.
- (c) If the numbering of the cosets of U/W is transferred to the zeroes of $\mathcal{R}_{U,P}(Y)$ then any permutation $\phi(\pi_{\sigma})$ induces a permutation of the zeroes which coincides with the permutation of the zeroes given by restricting the K-automorphism σ to M. By [Hupp67, I. 6.2], the kernel of the restricted map $\phi: G \to H$ is equal to D as given in (b), therefore $\phi(G)$ induces an isomorphism of $\operatorname{Gal}(M/k)$ with H.

We now explain how we will apply the preceding results in order to deal with the problem described in Section 6.2. We are given a Galois extension K/k defined by a polynomial A(Y) of degree m with Galois group $G \leq \mathfrak{S}_m$. Starting with some subgroup H of G, we look for a defining polynomial B(Y)of degree t for the extension K^H/k . Let

$$\mathcal{S} = \{ \overline{R}_G(x_1^{e_1} \cdot \ldots \cdot x_m^{e_m}) \mid e_1, \ldots, e_m \ge 0 \}$$

be the system of polynomials formed in terms of the modified Reynolds operator applied to the monomials. Then we have the equality of k-vector spaces

$$k[x_1,\ldots,x_m]^G = \bigoplus_{P \in \mathcal{S}} k \cdot P$$

generalizing the fact that any polynomial can be uniquely written as a sum of monomials. The representation of any element of $k[x_1, \ldots, x_m]^G$ in terms of

the elements of S is obtained from the solution of the corresponding system of k-linear equations which is formed by comparing coefficients.

We find a k-algebra basis of $k[x_1, \ldots, x_m]^G$ as a finite subset \mathcal{B} of \mathcal{S} which has the property that any element of \mathcal{S} can be written as some k-linear combination of products of powers of the elements of \mathcal{B} . By Theorem 6.3.1 we only have to consider elements of degree at most |G|, and by Proposition 6.3.1 the Molien series $\Phi_G(z)$ gives a hint to the degrees of the elements in \mathcal{B} .

We may calculate the image of any invariant $P \in k[x_1, \ldots, x_m]^G$ under the evaluation homomorphism ω_A by means of a resolvent polynomial. By Proposition 6.3.8, $\mathcal{R}_{\mathfrak{S}_m,P}(Y)$ has a non-repeated linear factor, say (Y - a). Then we have $\omega_A(P) = a$.

We finish this section by several remarks enlightening the importance of the described procedure.

Remark 6.3.3.

- 1. Our construction of defining polynomials via resolvent polynomials is sufficiently general. For let α be some primitive element of K^H over k. Suppose we are able to find some $P \in k[x_1, \ldots, x_m]^G$ with $\omega_A(P) = \alpha$. Then the minimal polynomial of α over k is equal to the resolvent polynomial $\mathcal{R}_{G,P}(Y)$.
- 2. We may ask how much smaller the degree of a defining polynomial is than the degree of its splitting field. By Theorem 6.3.4 and by the previous remark, the answer depends only on the structure of the group G. In particular, we notice the well-known fact that if the polynomial is of degree t, the degree of its splitting field is a divisor of t!.
- 3. If n is the number of subfields of K conjugate to K^H , we have the formula $n = (G : N_G(H))$, where $N_G(H)$ denotes the normalizer of H in G. If α denotes a primitive element of K^H over k, the value $\frac{t}{n} = (N_G(H) : H)$ is the number of conjugates of α which belong to K^H , hence which may be expressed as a polynomial in α with coefficients in k.

Thus, if we look for a polynomial B(Y) defining K/k whose degree is as small as possible, the preceding remarks suggest that we should consider subfields K^H of K which possess a large number of conjugate fields contained in K. We should get a polynomial B(Y) of fairly small degree if we find subgroups H of G with sufficiently small degree $(N_G(H) : H)$, preferably subgroups H with $N_G(H) = H$.

If on the other hand K/k is an abelian extension, any subgroup H of G satisfies $N_G(H) = G$. Therefore no abelian extension of degree d can be defined by some polynomial of degree strictly smaller than d.

6.4 Application to 4-Torsion Point Fields

The results of the preceding section are to be applied now in order to calculate a defining polynomial for the subfield L of the extension $k(x(E_4))/k$ (see Figure 5.7, page 82) by means of the strategy described in Section 6.2.

Our first task is to realize the Galois group of $k(x(E_4))/k$ as a subgroup of some suitable symmetric group. We use the operation of GL(2, n) on the points of order n in E_n to derive an operation of the factor group PGL(2, n)on the cyclic subgroups of order n of E_n . By numbering the subgroups we get an embedding of PGL(2, n) into $\mathfrak{S}_{\psi(n)}$ where $\psi(n)$ is defined in (5.7).

In our case n = 4, the considered group is $PGL(2, 4) = GL(2, 4)/\pm 1$. Its operation is uniquely described by permutations of pairs of points $\pm P$ for all points P of order 4 in E_4 . The realization of PGL(2, 4) as a subgroup G of \mathfrak{S}_6 is hence obtained by permuting the set $\{\pm P_1, \ldots, \pm P_6\}$, the notations being chosen as in Figure 6.1. The points having an order < 4 may be neglected.



Fig. 6.1. Points in E_4

If we consider $\{P_1, P_2\}$ as module basis, as it is indicated in Figure 6.1, and if we are given any matrix describing a module homomorphism, we may assign to it the corresponding permutation by tracing the images of the points. This assignment is unique up to selecting a module basis, i. e. up to conjugation in \mathfrak{S}_6 .

For the two generators $\pm \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$ of G we get

The permutations given above generate the image of $\operatorname{Gal}(k(x(E_4))/k)$ in \mathfrak{S}_6 which is a subgroup of G isomorphic to $\operatorname{Gal}(k(x(E_4))/k)$ of size 48 having exactly 15 conjugates within \mathfrak{S}_6 .

In order to realize the procedure described in Section 6.2 we first have to find a system of fundamental invariants of the algebra $k[x_1, \ldots, x_6]^G$ and then to calculate its image under the evaluation homomorphism ω_f .

 $k[x_1, \ldots, x_6]^G$ is a Cohen-Macaulay algebra of Krull dimension 6. Its Hilbert-series can be computed once we know the cycle types of all elements of G. The cycle types appearing in G are listed in Table 6.1, together with the numbers of the respective permutations.

Cycle Type	Number
(6)	8
(4,2)	6
(4,1,1)	6
(3,3)	8
(2,2,2)	7
(2,2,1,1)	9
(2,1,1,1,1)	3
(1,1,1,1,1,1)	1

Table 6.1. Cycle Types in PGL(2, 4)

If we substitute these values by means of Proposition 6.3.7 into the representation for the Hilbert-series $\Phi_G(z)$ according to Theorem 6.3.2 and expand the resulting expression by a polynomial of lowest possible degree so that the coefficients of all monomials appearing in the numerator become positive, we get the following formula for $\Phi_G(z)$

$$\Phi_G(z) = \frac{1+z^3+z^4+z^5+z^6+z^9}{(1-z)(1-z^2)^2(1-z^3)(1-z^4)(1-z^6)} .$$
(6.5)

Using this information we hope to find suitable primary and secondary invariants for a Hironaka decomposition (6.3). Success is not guaranteed for the degrees given by (6.5), but by Theorem 6.3.1, $k[x_1, \ldots, x_6]^G$ is generated by an algebra basis formed of homogenous invariants which may be computed by applying the Reynolds operator to monomials of degree ≤ 48 .

In the present situation there exists a suitable Hironaka decomposition whose invariants are images of monomials under the Reynolds operator. The decomposition is not unique, therefore we choose the monomials according to the rule that we should keep the maximal degree of any variable x_i as small as possible, so that the invariants are quite similar to elementary symmetric polynomials.

		Fundamenta	Image under ω_f		
u_1	=	$\overline{R}_G(x_1)$	=	$6R_G(x_1)$	0
u_2	=	$\overline{R}_G(x_2x_4)$	=	$3R_G(x_2x_4)$	a
v_2	=	$\overline{R}_G(x_1x_2)$	=	$12R_G(x_1x_2)$	4 a
u_3	=	$\overline{R}_G(x_1x_2x_3)$	=	$8R_G(x_1x_2x_3)$	-8 b
u_4	=	$\overline{R}_G(x_2x_3x_4x_5)$	=	$3R_G(x_2x_3x_4x_5)$	$-a^2$
u_6	=	$\overline{R}_G(x_1x_2x_3x_4x_5x_6)$	=	$R_G(x_1x_2x_3x_4x_5x_6)$	$-(a^3+8b^2)$
w_3	=	$\overline{R}_G(x_1x_2x_4)$	=	$12R_G(x_1x_2x_4)$	-12b
w_4	=	$\overline{R}_G(x_1x_2x_3x_4)$	=	$12R_G(x_1x_2x_3x_4)$	$-4 a^2$
w_5	=	$\overline{R}_G(x_1x_2x_3x_4x_5)$	=	$6R_G(x_1x_2x_3x_4x_5)$	4 a b

Table 6.2. Basis Invariants

The resulting invariants are listed in Table 6.2. They are computed by the modified Reynolds operator, so that they have integral coefficients.

 $\{u_1, u_2, v_2, u_3, u_4, u_6\}$ is a system of primary invariants, and the secondary invariants $\{1, w_3, w_3^2, w_3^3, w_4, w_5\}$ form a module basis of $k[x_1, \ldots, x_6]^G$ over $k[u_1, u_2, v_2, u_3, u_4, u_6]$. The fact that the primary invariants mentioned above are algebraically independent can be shown with the aid of Grobner bases (see [Stu93, 1.2.1 (4), Subroutine 2.5.3]). However, for the intended application it is only important that we are able to express all appearing invariants in terms of the generators.

The secondary invariants $\{w_3, w_4, w_5\}$ satisfy certain algebraic relations, called *syzygies*, which can be detected by calculating the basis representations of all products of elements of the module basis. The set of all syzygies forms an ideal in the polynomial ring $k[U_1, U_2, V_2, U_3, U_4, U_6, W_3, W_4, W_5]$ being the kernel of the homomorphism

$$k[U_1, U_2, V_2, U_3, U_4, U_6, W_3, W_4, W_5] \to k[x_1, \dots, x_6]^G,$$

 $U_i \mapsto u_i, V_i \mapsto v_i, W_i \mapsto w_i$.

The number and the degrees of the generators of the syzygy ideal can be read off from the Hilbert-series. The syzygies themselves satisfy certain algebraic dependencies which can be interpreted as the kernel of a homomorphism. Continuing this process, we get a free resolution of $k[x_1, \ldots, x_6]^G$ as a graded module. This procedure is carried out in Appendix E. In particular, we get for $k[x_1, \ldots, x_6]^G$ a free resolution of length 3.

Remark 6.4.1.

The results obtained above are valid in general only if the base field has a characteristic equal to 0 or prime to |G|. Regarding our case, in degree 6 the invariant

$$v_6 = \overline{R}_G(x_1^2 x_2 x_3 x_4 x_5) = 6R_G(x_1^2 x_2 x_3 x_4 x_5)$$

has the unique basis representation

$$3v_6 = u_2^2 v_2 - u_1 u_2 w_3 + u_1^2 u_4 + w_3^2 - u_2 w_4 - 4v_2 u_4 + 2u_1 w_5 - 18u_6,$$

so that v_6 cannot be expressed by the basis invariants listed above over any base field of characteristic 3.

In the next step of the procedure outlined in Section 6.2, we have to determine the images of the basis elements under the evaluation homomorphism ω_f . If u is a fundamental invariant then, by Proposition 6.3.3, the coefficients of the formal resolvent polynomial $\mathcal{RP}_{\mathfrak{S}_6}(u)(Y)$ are symmetric polynomials in x_1, \ldots, x_6 . They can therefore be expressed by elementary symmetric polynomials. Hence, $\mathcal{R}_{\mathfrak{S}_6,u}(Y)$ is a polynomial whose coefficients are polynomials in the coefficients of the defining polynomial of K, and $\omega_f(u)$ appears as a simple linear factor by Proposition 6.3.8.

Since some of the fundamental invariants or sums of them are already elementary symmetric functions, the total amount of computation reduces to the resolvent polynomials $\mathcal{R}_{\mathfrak{S}_{6},u}(Y)$ for $u = u_2, u_3, u_4$.

The methods for substituting terms and factorizing polynomials in existing computer algebra systems like Mathematica or MAPLE are not applicable in connection to our resolvent polynomials because they do not consider the inherent symmetry of the terms. We could not perform the arithmetic of invariants and the generation of basis representations within a reasonable amount of time on these systems because of the size of the appearing terms. We had therefore to develop a suitable program for these special purposes. Using this program we computed the basis representations of the coefficients of the considered formal resolvent polynomials. These data being used as input for Mathematica and MAPLE we substituted the elementary symmetric polynomials by the coefficients of the defining polynomial of $k(x(E_4)/k)$

$$A(Y) = \frac{1}{2}\Lambda_4(Y) = Y^6 + 5 a Y^4 + 20 b Y^3 - 5 a^2 Y^2 - 4 a b Y - a^3 - 8 b^2 ,$$

and factorized the resulting expressions.

The decompositions of the calculated resolvent polynomials into irreducible factors are given in Appendix D. The resulting values of the fundamental invariants under ω_f can be found in Table 6.2.
Once we have these values we may carry out the crucial step to calculating a defining polynomial. The subgroup H of G to be considered,

$$H = \{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \} \quad \longleftrightarrow \quad \{ (), (1, 6)(2, 4)(3, 5) \} ,$$

is a normal subgroup, the factor group N = G/H as an abstract group being isomorphic to \mathfrak{S}_4 . Hence the polynomial to be determined should have degree 4. Consequently we are looking for a subgroup F of G, so that its projection \overline{F} into N has exactly 4 conjugates within N.

We conclude that the normalizer of \overline{F} in N needs to have index 4 in N. Since N is isomorphic to \mathfrak{S}_4 , the normalizer described above is isomorphic to \mathfrak{S}_3 , and we discover suitable F having sizes 6 and 12, respectively. In order for the resolvent polynomial to have degree 4 we require |F| = 12. Since all of the 4 possible subgroups F lead to the same resolvent polynomials, we may select any of these groups as our F, for example

$$F = \{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}, \pm \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}, \\ \pm \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}, \pm \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \pm \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}, \pm \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix}, \pm \begin{pmatrix} -1 & 1 \\ 1 & 2 \end{pmatrix}, \pm \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \}$$

F is generated by

$$\{\pm \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\} \quad \longleftrightarrow \quad \{(1, 2, 5, 6, 4, 3), (1, 4)(2, 6)\}.$$

A system of representatives of G/F is given by

$$\{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\} \quad \longleftrightarrow \quad \{(), (1, 6), (2, 4), (3, 5)\}.$$

Finally, we need a polynomial $P \in k[x_1, \ldots, x_6]$ having stabilizer subgroup $\operatorname{Stab}_G(P) = F$ which should be homogenous and of lowest possible degree. There is no suitable polynomial in degree 1, but in degree 2 we find

$$P = \overline{R}_F(x_1 x_2).$$

The defining polynomial we are looking for is the resolvent polynomial with respect to G and P. Its calculation is performed similar to our procedure to determine the images of the basis elements under ω_f . Fortunately, the effort is much smaller since the resolvent polynomial has degree 4 instead of 15 with respect to Y. Therefore we give here the essential intermediate results as an example for all computed resolvent polynomials. The formal resolvent polynomial has the form

$$\begin{aligned} \mathcal{RP}_{G}(P)(Y) &= Y^{4} - \overline{R}_{G}(2\,x_{1}x_{2})\,Y^{3} \\ &+ \overline{R}_{G}(x_{1}^{2}x_{2}^{2} + 3\,x_{1}^{2}x_{2}x_{3} + 4\,x_{1}^{2}x_{2}x_{4} + 6\,x_{1}x_{2}x_{3}x_{4} + 4\,x_{2}x_{3}x_{4}x_{5})\,Y^{2} \\ &- \overline{R}_{G}(x_{1}^{3}x_{2}^{2}x_{3} + 2\,x_{1}^{3}x_{2}^{2}x_{4} + 4\,x_{1}^{3}x_{2}x_{3}x_{4} + 2\,x_{1}^{2}x_{2}^{2}x_{3}^{2} + 5\,x_{1}^{2}x_{2}^{2}x_{3}x_{4} \\ &+ 8\,x_{1}^{2}x_{2}x_{3}^{2}x_{4} + 4\,x_{2}^{2}x_{3}^{2}x_{4}x_{5} + 8\,x_{1}^{2}x_{2}x_{3}x_{4}x_{5} + 8\,x_{1}x_{2}^{2}x_{3}x_{4}x_{5} \\ &+ 32\,x_{1}x_{2}x_{3}x_{4}x_{5}x_{6})\,Y \\ &+ \overline{R}_{G}(x_{1}^{4}x_{2}^{2}x_{4}^{2} + x_{1}^{4}x_{2}^{2}x_{3}x_{4} + x_{1}^{4}x_{2}x_{3}^{2}x_{4} + 2\,x_{1}^{4}x_{2}x_{3}x_{4}x_{5} + x_{1}^{3}x_{2}^{2}x_{3}x_{4} \\ &+ 2\,x_{1}^{3}x_{2}x_{3}^{3}x_{4} + 2\,x_{2}^{3}x_{3}^{3}x_{4}x_{5} + 3\,x_{1}^{3}x_{2}^{2}x_{3}x_{4} + 2\,x_{1}^{2}x_{2}^{2}x_{3}x_{4}x_{5} + 3\,x_{1}x_{2}^{2}x_{3}x_{4}x_{5} + 3\,x_{1}x_{2}^{2}x_{3}^{2}x_{4} \\ &+ 2\,x_{1}^{3}x_{2}x_{3}x_{4}x_{5}x_{6} + 2\,x_{1}^{2}x_{2}^{2}x_{3}^{2}x_{4}^{2} + 4\,x_{2}^{2}x_{2}^{2}x_{4}^{2}x_{5}^{2} + 6\,x_{1}^{2}x_{2}^{2}x_{3}^{2}x_{4}x_{5} \\ &+ 8\,x_{1}^{2}x_{2}x_{3}x_{4}^{2}x_{5} + 4\,x_{1}x_{2}^{2}x_{3}^{2}x_{4}^{2}x_{5} + 14\,x_{1}^{2}x_{2}^{2}x_{3}x_{4}x_{5}x_{6} \\ &+ 4\,x_{1}x_{2}^{2}x_{3}x_{4}^{2}x_{5} + 6\,x_{1}x_{2}x_{3}x_{4}^{2}x_{5}x_{6} \end{aligned}$$

The representation by basis functions is as follows

$$\begin{aligned} \mathcal{RP}_{G}(P)(Y) &= Y^{4} - 2v_{2}Y^{3} + (v_{2}^{2} + u_{1}u_{3} + 2u_{1}w_{3} - 2u_{2}v_{2} - 2w_{4} - 8u_{4})Y^{2} \\ &-(u_{1}v_{2}u_{3} + 2u_{1}v_{2}w_{3} - 2u_{2}v_{2}^{2} + \frac{16}{3}u_{1}u_{2}w_{3} - \frac{16}{3}u_{2}^{2}v_{2} \\ &-\frac{16}{3}u_{1}^{2}u_{4} - u_{3}^{2} - \frac{16}{3}w_{3}^{2} + 2v_{2}w_{4} - 4u_{3}w_{3} + \frac{16}{3}u_{2}w_{4} \\ &+ \frac{40}{3}v_{2}u_{4} - \frac{32}{3}u_{1}w_{5} + 64u_{6})Y \\ &+(2u_{1}^{3}u_{2}w_{3} - 2u_{1}^{2}u_{2}^{2}v_{2} - 2u_{1}^{4}u_{4} - \frac{16}{3}u_{1}u_{2}^{2}w_{3} + \frac{16}{3}u_{3}^{2}v_{2} - u_{1}^{2}w_{3}^{2} \\ &- \frac{7}{3}u_{1}u_{2}v_{2}w_{3} + \frac{4}{3}u_{2}^{2}v_{2}^{2} + u_{1}^{2}v_{2}w_{4} - u_{1}u_{2}v_{2}u_{3} + 2u_{1}u_{2}^{2}u_{3} \\ &+ \frac{25}{3}u_{1}^{2}v_{2}u_{4} + \frac{16}{3}u_{1}^{2}u_{2}u_{4} - 2u_{1}^{3}w_{5} + \frac{1}{3}v_{2}w_{3}^{2} + \frac{16}{3}u_{2}w_{3}^{2} \\ &- \frac{16}{3}u_{2}^{2}w_{4} - \frac{4}{3}v_{2}^{2}u_{4} - u_{1}u_{3}w_{4} + u_{2}u_{3}^{2} - \frac{4}{3}u_{2}v_{2}w_{4} + 3u_{2}u_{3}w_{3} \\ &- 8u_{1}w_{3}u_{4} - \frac{40}{3}u_{2}v_{2}u_{4} - \frac{7}{3}u_{1}v_{2}w_{5} - 9u_{1}u_{3}u_{4} - 9u_{1}u_{3}u_{4} \\ &+ \frac{32}{3}u_{1}u_{2}w_{5} + 16u_{1}^{2}u_{6} + 16u_{4}^{2} + 3u_{3}w_{5} + 8u_{4}w_{4} - 64u_{2}u_{6}) \end{aligned}$$

If we substitute the values of the basis invariants (see Table 6.2), we get $\mathcal{R}_{G,P}(Y) = Y^4 - 8 a Y^3 + 24 a^2 Y^2 + (224 a^3 + 1728 b^2) Y + 272 a^4 + 1728 a b^2.$

After performing the linear substitution $Y \mapsto Y + 2a$ and introducing the quantity $\Delta = -16(4a^3 + 27b^2)$ (the discriminant of the underlying elliptic curve) we obtain as a defining polynomial of the extension L/k

$$B(Y) = Y^{4} + (256 a^{3} + 1728 b^{2}) Y + 768 a^{4} + 5184 a b^{2}$$

= Y⁴ - 4 \Delta Y - 12 a \Delta . (6.6)

Remark 6.4.2.

If we apply the procedure described above to the subgroup F' satisfying |F'| = 16 which is given by

$$F' = \langle \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rangle \longleftrightarrow \langle (1, 6)(2, 5, 4, 3), (2, 5, 4, 3), (3, 5) \rangle$$

having the system of representatives for G/F'

$$\{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \pm \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}\} \quad \longleftrightarrow \quad \{(), (1, 5, 6, 3), (1, 2, 6, 4)\}$$

and if we choose the invariant $P = \overline{R}_{F'}(x_1) = x_1 + x_6$, we calculate the resolvent polynomial

$$\mathcal{RP}_G(P)(Y) = Y^3 - u_1 Y^2 + v_2 Y - u_3 ,$$

 $\mathcal{R}_{G,P}(Y) = Y^3 + 4 a Y + 8 b,$

such that after a linear substitution, we rediscover the known polynomial $\Lambda_2(Y) = 2(Y^3 + aY + b)$ defining the subextension $k(E_2)/k$.

The above example illustrates that we may assume that the shape of the calculated polynomial $B(Y) = Y^4 - 4\Delta Y - 12a\Delta$ is quite good with respect to the size and the homogenous degree of the coefficients. On the other hand, the polynomial B(Y) is not optimal for describing the extension L/k as its discriminant is given by

$$Dis(B) = 2^{12} 3^6 b^2 \Delta^3$$
,

and compared to $\text{Dis}(\Lambda_4) = -2^8 \Delta^5$ we observe additional factors of the discriminant which result from the divisors of 3 and b.

There are no suitable polynomial invariants P of degree 1, however, and if we increase the degree of P, we encounter even more additional divisors or higher exponents of the factors in the corresponding discriminant.

If we want to get to possibly better results then we have to give up our restriction to homogenous polynomials P and include more general invariants into our examination. We have two fundamental ways to do this:

- We abandon the homogenity of the polynomials,
- We investigate rational invariants, i. e. $P \in k(x_1, \ldots, x_6)^G$.

Both approaches can in principle be treated by the programs described above, for example by reducing the calculations to the homogenous components or by multiplying out the denominators, but the number of possible invariants P is increasing quite rapidly, so that we need a good strategy to limit ourselves to the consideration of invariants which lead to reasonable results.

A Invariants of Elliptic Modular Curves

An elliptic modular curve is a modular curve $X_0(N)$ of genus 1. Using Proposition 4.1.3 (see Section 4.1) one infers that the genus of the elliptic modular curves $X_0(N)$ equals 1 exactly for the following 12 values of N

N = 11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49.

The curves determined by these values of N have complex multiplication exactly for N = 27, 32, 36, 49. Consequently, the remaining 8 values of Nprovide those elliptic modular curves without complex multiplication which are to be considered. For these curves defined over \mathbb{Q} , Ligozat [Ligo75, 4.2] has calculated a minimal equation. Their coefficients are given below.

N	a_1	a_3	a_2	a_4	a_6	g_2	g_3	Δ	j
11	0	1	-1	-10	-20	$\frac{2^2 \cdot 31}{3}$	$\frac{41 \cdot 61}{3^3}$	-11^{5}	$-\frac{2^{12}\cdot 31^3}{11^5}$
14	1	1	0	4	-6	$-rac{5\cdot43}{2^2\cdot3}$	$\frac{11\cdot 13\cdot 37}{2^3\cdot 3^3}$	$-2^6 \cdot 7^3$	$\frac{5^3 \cdot 43^3}{2^6 \cdot 7^3}$
15	1	1	1	-10	-10	$\frac{13\cdot 37}{2^2\cdot 3}$	$\frac{7 \cdot 17 \cdot 41}{2^3 \cdot 3^3}$	$3^4 \cdot 5^4$	$\frac{13^3 \cdot 37^3}{3^4 \cdot 5^4}$
17	1	1	-1	-1	-14	$\frac{11}{2^2}$	$\frac{5 \cdot 89}{2^3}$	-17^{4}	$-rac{3^3\cdot11^3}{17^4}$
19	0	1	1	-9	-15	$\frac{2^4 \cdot 7}{3}$	$\frac{13 \cdot 97}{3^3}$	-19^{3}	$-rac{2^{18}\cdot7^3}{19^3}$
20	0	0	1	4	4	$-\frac{2^2 \cdot 11}{3}$	$-\frac{2^{3}\cdot 37}{3^{3}}$	$-2^8 \cdot 5^2$	$\frac{2^4 \cdot 11^3}{5^2}$
21	1	0	0	-4	-1	$\frac{193}{2^2 \cdot 3}$	$\frac{5^2 \cdot 23}{2^3 \cdot 3^3}$	$3^4 \cdot 7^2$	$\frac{193^3}{3^4 \cdot 7^2}$
24	0	0	-1	-4	4	$\frac{2^2 \cdot 13}{3}$	$-\tfrac{2^3\cdot 5\cdot 7}{3^3}$	$2^8 \cdot 3^2$	$\frac{2^4 \cdot 13^3}{3^2}$

Table A.1. Parameters of the Curves $X_0(N)$

© Springer-Verlag Berlin Heidelberg 2001

The parameters in Table A.1 refer to equations of the following forms:

$$y^{2} + a_{1}xy + a_{3}y = x^{3} + a_{2}x^{2} + a_{4}x + a_{6}$$
(A.1)

and

$$y^2 = 4x^3 - g_2x - g_3. \tag{A.2}$$

Each of the equations of the form (A.1) with coefficients taken from Table A.1 is a minimal equation over \mathbb{Q} because all prime numbers p satisfy the inequality $v_p(\Delta) < 12$ (see [Silv86, VI. 1.1]). Despite its exceptional position, such a minimal equation is generally not unique, since any transformation $(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t)$ with $r, s, t \in \mathbb{Q}$ and $u = \pm 1$ provides another minimal equation if the resulting coefficients a_i are elements of \mathbb{Z} .

All elliptic modular curves $X_0(N)$ considered in Table A.1 have no complex multiplication because their *j*-invariants are not integral.

Rathmann [Rath88] has determined which elliptic modular curves $X_0(N)$ are semistable and for which prime numbers ℓ the respective ℓ -adic representations $\varrho_{\ell} : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{Aut} T_{\ell}(X_0(N))$ are not surjective. The results are summarized in Table A.2.

N	11	14	15	17	19	20	21	24
ℓ with ϱ_ℓ not surjective	5	2, 3	2	2	3	2, 3	2	2
$X_0(N)$ semistable	у	у	у	у	у	n	у	n

Table A.2. Non-Surjectivity of ρ_{ℓ} and Semistability of $X_0(N)$

B L-series Coefficients a_p

The L-series coefficients of those elliptic modular curves $X_0(N)$ without complex multiplication given in the tables below were computed in [Adel94]. They were calculated by several simple procedures, for example

- The expansion of products of the η -function (cf. Table 4.1) applied in those cases where the unique normalized cusp form in $S_2(\Gamma_0(N))$ has a representation of the appropriate shape.
- The evaluation of the formula

$$a_p = -\sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right),$$

if $y^2 = f(x)$ is a defining equation (A.2) of the curve.

There are more efficient methods for the computation of L-series coefficients of arbitrary elliptic curves (see [Cohe93, 7.4.3]). For simplicity reasons, we did not use these procedures. The calculated values just served as a basis to verify various assertions against numerical data. The following tables contain only a minute part of the actually computed coefficients.

 $[\]bigodot$ Springer-Verlag Berlin Heidelberg 2001

				1	V									1	V			
<i>p</i>	11	14	15	17	19	20	21	24		<i>p</i>	11	14	15	17	19	20	21	24
2	-2	-1	-1	-1	0	0	-1	0		233	24	-6	-6	-6	-21	-6	-6	10
3	-1	-2	-1	0	-1	-2	1	-1		239	-30	24	-16	-16	15	-24	24	-16
5	1	0	1	-2	3	-1	-2	-2		241	-8	-10	-14	18	-10	14	2	18
	-2	1	0	4	-1	2	-1	0		251	-23	-18	12	12	21	0	-20	20
11	1	0	-4	0		0	4	4		257	-2	18	18	18		-6	26	2
13	4	-4	-2	-2	-4		-2	-2		263	14	0	16	-16	9	-18	16	-8
17	-2	6			-3	-6	-6	2		269	10	-12	14	22	24	18	6	-10
19	0			-4		-4	4	-4		271	-28	-16	16	-10	-10	20	16	8
23	-1					6	0	-8 6		277	-2	-10			-19	20	22	-20
29		-0	-2				-2	0		201	-10	-0	-0	-0 1 <i>C</i>	10		-22	20
01 97	1	-4		4	-4	-4	6	0		200	4 94	-22	-12	-10	10	20	-20	-20
11	2		10	-2	6	6	2	6		293	24	24	28	12	20	-30	14	-10
13	-6	8			-0	_10	_1	-0		311	12	_24	-24	28	20	12	-24	-24
47	8	-12	8	0	-3	-6	0	0		313	1	_10	26	-22	-10	-22	26	-6
53	-6	6	-10	6	12	-6	6	-2		317	13	6	-2	-10	6	-6	-18	6
59	5	-6	-4	-12	-6	12	12	4		331	7	8	12	4	-28	8	-4	20
61	12	8	-2	-10	-1	2	-2	-2		337	-22	14	-14	-14	32	2	-14	18
67	-7	-4	12	4	-4	2	4	-4		347	28	-24	-28	32	21	-30	-28	-12
71	-3	0	-8	-4	6	-12	0	8		349	30	-28	-2	-18	17	-10	-2	30
73	4	2	10	-6	-7	2	-6	10		353	-21	18	18	-30	-6	18	10	2
79	-10	8	0	12	8	8	-16	-8		359	-20	-24	-24	0	15	24	32	-24
83	-6	-6	12	-4	12	6	-12	-4		367	-17	8	-24	28	8	-22	0	-8
89	15	-6	-6	10	12	-6	-14	-6		373	-26	14	-26	6	-4	26	-10	-10
97	-7	-10	2	2	8	2	18	2		379	-5	-16	-20	-8	-34	-28	12	20
101	2	0	6	-10	6	6	14	-18		383	-1	36	-24	-24	12	6	0	0
103	-16	-4	-16	8	14	14	8	16		389	-15	18	6	6	15	-6	6	-2
107	18	12	-12	8	-18	-6	4	-12		397	-2	20	-2	6	-7	2	-18	14
109	10		14	6	-16		-18	-2		401	2	-18	18	-14	12	-30	-30	-30
113	9	0 10		-14	6	-6	-14	18		409	-30		26	26	-4	-34	-22	-0 10
$121 \\ 191$	10	-10	-0	16			0	-0		419	20	10	4	0	-12	30	-12	12
$\frac{131}{137}$	-10	10	-12	10	-10	18	4	-4		421	18	-10	-20	12	$\begin{vmatrix} 0\\ 24 \end{vmatrix}$	20	30	-10
137	10	1/	-0	-0	12	10	-0 19	-0		401	-10	24	14	12	-24	30	-24	14
149	-10	-18	$\frac{-1}{22}$	-10	21^{-10}	-6	6	14		439	40	-54	40^{-14}	-20	-10	8	-24	-14
151	2	8	-8	-16	-10	20	8	-16		443	-11	-12	-12	28	-3	6	36	20
157	-7	-4	14	-2	14	-22	-2	-2		449	35	18	2	$\frac{-0}{34}$		6	-30	-14
163	4	-16	-4	24	20	-10	4	12		457	-12	-10	10	-6	-37	26	10	-22
167	-12	-12	0	-4	-18	18	-8	24		461	12	12	-18	-2	9	30	-10	-26
173	-6	-12	-18	22	-18	-6	-10	6		463	-11	32	24	32	-31	14	16	8
179	-15	-12	20	12	-18	-12	-4	12		467	-27	-6	28	12	-27	-30	36	-36
181	7	20	-10	-2	2	-10	-26	6		479	20	-36	0	36	-12	-24	-16	-16
191	17	24	16	-16	3	-12	-8	0		487	23	-16	32	20	2	26	-8	-32
193	4	14	2	2	-4	26	2	2		491	-8	-12	28	20	12	0	20	-12
197	-2	-18	6	-18	18	18	22	-18		499	20	-4	4	-40	5	-4	4	12
199	0	20	-8	-20	11	8	24	16		503	-26	0	-32	-12	12	-18	24	24
211	12	-4	20	8	14	-16	4	-20		509	15	36	-34	-2	0	6	-10	6
223	19	8	8	24	-10	-10	16	-8		521	-3	6	10	26	0	-6	18	26
227	18	18	-20	-24	12	-6	-12	12		523	-16	$\begin{vmatrix} 2 \\ c \\$	4	-36		14	-20	4
229	15	-4	6	6	5	14	-10	22	J	541	-8	38	30	6	-25	14	-34	-18

				1	V							
p	11	14	15	17	19	20	21	24		p	11	
547	8	8	-20	-32	-28	26	4	44		877	-12	-
557	-2	6	-18	30	21	-30	-2	-26		881	-43	
563	4	30	12	-4	6	-18	4	28		883	4	
569	0	6	-6	-38	-24	30	10	10		887	-22	-
571	-28	32	-4	-32	-4	8	-4	36		907	-12	
577	33	2	2	-14	11	-22	34	2		911	12	
587	28	-42	-12	4	45	-6	28	-44		919	10	
593	44	-6	34	18	-42	18	-6	-14		929	-30	
599	40	-24	-8	-24	-36	0	48	24		937	8	
601	2	26	26	10	26	-10	-6	-38		941	42	
607	-22	32	-8	20	32	-22	-16	-40		947	-27	
613	-16	2	22	-26	29	2	-26	38		953	34	.
617	18	6	-6	-6	9	-6	-6	42		967	-32	
619	-25	26	-4	-48	44	20	-20	-44		971	47	
631	7	-16	-8	16	11	-28	-40	16		977	-27	
641	-33	-18	-30	-30	0	-18	18	-14		983	39	
643	29	14	-36	32	-13	14	20	12		991	-8	
647	-7	-12	32	8	27	42	-40	8		997	38	
653	-41	18	46	6	-39	42	-18	6		1009	-10	
659	10	-24	20	4	-30	36	12	12		1013	39	
661	37	-40	22	38	32	-22	22	-10		1019	-10	
673	14	26	-30	2	-10	-46	34	34		1021	22	
677	-42	-12	6	30	-42	18	-18	-2		1031	32	
683	-16	-12	36	-40	36	-42	-12	4		1033	-16	
691	17	-46	-44	-8	17	8	20	-4		1039	5	
701	2	18	-2	-18	6	-30	30	6		1049	-55	
709	-25	-46	-26	-34	26	-34	6	-10		1051	2	
719	15	12	-48	4	15	-24	-48	-32		1061	-13	
727	3	44	-16	40	-19	-46	-40	48		1063	44	
733	-36	-40	14	-50	-22	-22	-18	14		1069	-20	
739	50	-16	-44	28	11	20	36	-4		1087	8	
743	4	24	-16	12	-24	6	0	-8		1091	-58	
751	-23	-40	16	20	32	-4	-32	24		1093	-51	
757	-22	2	-26	$\frac{-0}{22}$	-25	-22	-10	38		1097	-42	
761	12	-18	-6	-22	33	42	18	-22		1103	-51	
769	20	14	$\frac{1}{2}$	-14	23	2	2	2		1109	-30	
773	-6	24	6	-26	-6	-30	14	-18		1117	48	
787	-32	-22	28	-32	-4	26	-44	28		1123	24	
797	53	-12	-2	-50	-12	42	-26	22		1129	50	
809	0	6	10	26	_9	-6	42	26		1151	2	
811	-38	2	12	40	-16	-16	44	4		1153	-31	
821	22	6	54	-18	33	-54	38	30		1163	34	
823	30	_40	32	20	0	38	24	-16		1171	-3	ſ
827	-52	-36	22	_18	19	_30	_19	-28		1181	-18	1
820	25	56	20	21	16	-00 0	11	_50		1187	19	
830	20	19	10	204	18	_18		-30		1102		ľ
852	14	14	0+0 6	14	26	50	_10	_10		1201	21	
857	Q 14	10	20	10	10	19	14	19		1912		
001	15	14	-44	10	10	10	-14	12		1017	40	1
009	-15	14	-20	02 10	-49	-4	44	-12		1211	-42	
803	24	-24	-90	16	18	6	-24	-32	J	1223	14	1-

				1	V			
p	11	14	15	17	19	20	21	24
877	-12	-22	30	6	-22	26	46	-18
881	-43	-54	-46	-46	-27	-18	-6	50
883	4	20	44	-12	47	14	-28	-4
887	-22	-36	48	12	18	18	8	8
907	-12	44	-12	32	8	-46	-4	4
911	12	48	32	-4	-6	12	-24	16
919	10	56	40	24	20	-16	8	16
929	-30	6	34	-30	-18	-42	26	50
937	8	2	-54	10	-7	-22	42	42
941	42	-24	-50	6	-18	-18	38	6
947	-27	24	-36	32	-36	18	44	12
953	34	-54	-22	-22	-48	-6	26	-54
967	-32	32	32	0	-40	-22	40	-16
971	47	-6	60	-12	60	-24	12	36
977	-27	-6	2	18	24	18	-30	-30
983	39	-36	0	12	-36	-18	24	-24
991	-8	-16	32	-12	-34	-4	-16	40
997	38	8	54	46	17	26	-26	-26
009	-10	-34	50	-14	$\frac{1}{20}$	50	-14	-46
013	39	-36	22	30	-0	18	-34	-50
019	-10	36	-36	-36	30	36	-12	36
021	22	-4	-2	14	-40	14	30	30
031	32	0	24	-12	-24	12	0	-40
033	-16	26	-54	58	26	2	-22	10
039	5	-4	-32	40	-4	-16	32	-40
049	-55	-30	-6	-22	27	42	2	26
051	2	44	60	8	44	8	28	-28
061	-13	-30	6	-18	33	54	-26	30
1063	44	-16	-16	-48	56	-10	-24	16
1069	-20	8	-50	-50	-1	-46	46	14
1087	8	8	-40	0	-19	-22	32	8
091	-58	30	-44	0	-24	48	-60	-52
1093	-51	-22	22	62	-58	-22	38	54
1097	-42	-6	58	42	6	-30	-46	-54
103	-51	48	24	8	-57	-42	24	48
109	-30	36	-10	6	-15	30	-34	-18
117	48	-34	-18	-26	-34	-46	-2	-50
123	24	-46	28	36	26	14	4	-36
129	50	50	-22	-38	50	62	10	10
151	2	-12	-16	-12	36	12	-32	0
153	-31	2	34	2	-34	-22	-14	-62
163	34	-60	-28	-16	-57	54	-60	-12
171	-3	20	-12	28	56	-40	-28	-20
181	-18	60	-34	-34	-18	-30	6	22
187	-12	-12	12	0	48	-6	28	-36
193	-21	66	-38	26	36	-6	18	-22
201	2	14	-14	-14	5	14	50	-14
213	-41	26	-18	-10	-46	26	30	46
217	-42	-6	18	66	30	-30	-6	2
1223	14	-24	16	-56	45	30	24	24

				1	V								1	V			
p	11	14	15	17	19	20	21	24	p	11	14	15	17	19	20	21	24
1229	60	30	-18	-10	36	6	-34	38	1597	-32	-58	-50	-2	50	50	-34	78
1231	-18	-28	48	-36	-10	-28	32	8	1601	2	66	2	34	51	18	42	-30
1237	18	-40	6	-10	-40	-22	6	38	1607	33	48	0	16	60	-6	64	8
1249	40	26	34	-14	-10	-46	-14	34	1609	-10	26	-54	26	-64	14	58	10
1259	-25	18	12	-20	60	60	44	-60	1613	-6	-72	46	-18	-9	-6	22	54
1277	-47	24	30	-34	21	-6	-58	6	1619	-20	-60	-12	4	12	12	44	12
1279	-15	20	-16	16	-7	32	-48	56	1621	22	74	22	-2	29	-58	-10	38
1283	-36	0	-4	60	0	30	-36	12	1627	78	-10	-28	-8	26	-46	12	4
1289	0	30	42	-6	9	-6	42	-22	1637	33	0	6	-2	-66	42	-18	78
1291	-8	-58	44	44	14	56	28	4	1657	-2	-34	26	-22	-70	-70	26	58
1297	48	-34	-46	-46	2	26	18	18	1663	4	8	-56	36	-46	38	32	-8
1301	27	-48	22	54	18	42	-18	-18	1667	48	48	-20	-60	-54	42	-52	60
1303	39	8	0	36	-1	14	-56	-32	1669	50	32	38	-2	-13	14	-10	22
1307	28	42	-28	-60	60	-6	28	-28	1693	-6	56	-18	-10	74	50	-34	-66
1319	-30	-24	-24	4	-66	-48	-40	8	1697	-42	-42	-78	-62	-9	42	-22	-14
1321	47	62	-22	-38	-10	-10	10	-22	1699	40	-10	52	36	-64	44	-28	-4
1327	68	32	-56	16	32	50	-64	-40	1709	-45	54	14	-2	36	6	-66	38
1361	12	-18	18	18	-60	18	-38	-62	1721	-3	-6	58	58	39	42	-62	26
1367	-72	-24	16	-12	-36	18	-32	-24	1723	-46	-4	20	-80	-22	-58	28	-76
1373	39	-30	-66	-50	-33	18	30	54	1733	-6	-6	-58	6	-45	-78		62
1381	-68	-22	-26	-58	14	26	38	-10	1741	17	-76	14	6	32	62	-50	-50
1399	60	-40	8	-36	14	32	-8		1747	-57	56	28	4	-34	$\begin{vmatrix} 2 \\ 2 \end{vmatrix}$	68	-52
1409	-15	18	-30	66	66	18	2	18	1753	34	-46	26	58	17	26	10	-38
1423	29	56	-8	-28	-7	-34	32	8	1759	-40	32	48	-56	-49	-16	-16	40
1427	-12	-30	28	20	-42	-54	20	60	1777	8	50	18	-14	32	-22	-62	-14
1429	-70	26	-10	-26		-22	-10	-10	1783	59	-16	-64	-16	50	-58	50	-64
1433	54	42	-54	42	-0	-30	-14	-0	1700	-57	12	30	30	-21	18	52	-12
1439		24	64	60	24		8	48	1789	10	-10	30	46	44	-10	30	62 10
1447	28	-04	-32	32	02	-22	10	48	1801	02	-34	-54	38	-34	38		10
1401	32	-40	-30	60	50	-24	-12	02 66	1011		42	-00	10	10	-40	64	70 80
1400	-11	- 00 - 20	30	16	59	-40	40	-00	1020	-30	-24	40 56	-40	42	-42	-04	-00 16
1409	-20	- 00 - 20	64	-10	-52	-52	16	40	1031	-40	-40	-50	12	-4	49	-24	10
14/1	22	52	-04	6	30	54	10	10	1861	-52	12	-00	10	10	42	-40	-0 58
1401	10	-0	-22	68	55	62	36	60	1867	28	50	12	24	-10	-38	10	-00 28
1400	58	04-	-20	-00	-55	30	-30	64	1871	20	18	-12	18	-43	36	24	16
1480	_15	-58	18	50	-40	-58	-62	50	1873		10	_14	18	25	26	89	50
1/03	-10	30	-74	14	$-51 \\ -27$	12	38	-50	1877	18	78	5/	-66	-20	_30	6	_18
1499	55	-12	-36	-24	-24	-60	36	20^{-50}	1879	-35	44	8	32	-30	80	56	-16
1511	37	12	-72	-32	-60	60	8	40	1889	70	18	-30	-14	72	-42	-6	2
1523	-41	-72	12	-56	-54	54	60	-36	1901	77	-18	46	-42	-42	18	-2	-26
1531	32	2	-36	-4	-7	-64	-36	-28	1907	-52	42	28	-48	27	$\frac{10}{42}$	52	$\frac{20}{12}$
1543	-36	32	16	24	-40	-10	-72	64	1913	-36	54	-54	-22	72	18	-54	-38
1549	-15	-34	-18	-18	38	-10	46	46	1931	-18	-30	-36	80	-30	48	60	-12
1553	-56	42	66	18	66	-30	-54	18	1933	54	62	-34	54	26	26	-50	-18
1559	-60	-12	56	28	21	24	40	-40	1949	-40	84	30	54	-30	18	-26	-74
1567	-52	-16	56	-28	-43	50	-32	-56	1951	-23	-64	32	-48	8	-52	-80	-40
1571	-28	66	20	-8	0	-72	20	60	1973	79	-60	-42	6	-9	-78	14	-66
1579	-30	-40	-4	52	32	-4	-20	52	1979	30	30	60	64	-48	-60	-52	-12
1583	34	0	56	-24	21	78	24	-16	1987	-22	-82	44	44	-19	-46	68	44

				Ι	V				N									
<i>p</i>	11	14	15	17	19	20	21	24		p	11	14	15	17	19	20	21	24
1993	-66	14	42	-6	-31	50	-54	74		2371	-28	14	36	-36	-22	80	52	-84
1997	-72	-78	14	78	6	-54	-18	-58		2377	3	-70	-54	-38	-52	74	-54	-22
1999	-20	-16	-32	-4	-25	-88	-80	-40		2381	-18	-66	-50	78	27	-78	-2	22
2003	4	-48	12	-48	24	-18	-20	-20		2383	-36	-28	88	-76	62	62	96	-24
2011	-13	-40	28	-40	5	32	60	84		2389	-50	14	54	-10	-40	-34	22	-10
2017	-17	-70	2	2	20	2	66	2		2393	54	18	42	-54	72	-78	2	26
2027	63	-72	-12	-68	-12	66	-12	36		2399	-75	-36	64	-40	48	72	0	64
2029	45	32	14	-26	14	-10	30	-34		2411	62	42	-36	-8	-12	-72	12	-76
2039	60	0	24	-72	-45	24	-80	56		2417	-22	18	66	18	-63	-78	-46	34
2053	84	38	54	38	74	2	-26	-58		2423	-31	48	32	0	78	54	-48	-24
2063	24	24	24	-20	3	54	-48	48		2437	-82	62	22	-18	-55	74	6	38
2069	70	-30	54	-82	-30	30	-10	30		2441	42	-30	74	-70	42	-54	-62	42
2081	-18	42	-30	66	-48	-30	18	-46		2447	3	-48	-24	48	30	-54	-24	48
2083	89	32	-4	-4	-58	-82	-12	-20		2459	-50	60	-4	48	48	-36	-76	20
2087	48	0	-32	-40	-48	-30	-16	-8		2467	3	2	-52	12	-7	-70	-28	-68
2089	-10	-70	-86	10	-16	74	26	-22		2473	-11	-10	10	-54	-46	74	-86	42
2099	35	30	-12	-20	-3	-36	-12	-84		2477	48	84	-18	-74	-78	-30	-58	-42
2111	-38	48	-48	4	48	12	-24	48		2503	14	-16	-48	-72	74	-34	40	-32
2113	-86	26	-30	34	-1	26	-14	$\frac{2}{-2}$		2521	72	38	26	74	-16	-10	90	-38
2129	20	-30	18	18	-3	-42	66	-78		2531	57	36	84	-52	-12	48	12	-52
2131	-68	-10	20	56	62	8	-28	-20		2539		-34	-36	64	74	68	-36	36
2137	73	50	-70	42	41	$\begin{vmatrix} 2 \\ 0 \end{vmatrix}$	-38	-38		2543		0	-40	-36	-15	78	72	80
2141	-58	-72	-34	-34	66	-30	6	-58		2549	-20	30	54	6	-54	90	-90	-2
2143	-91	56	-56	64	-16	-34	-16	-50		2551	-98	-40	24	-72	59	-76	50	16
2153	-26	54	-0	-6	6	-30	42	58		2557	13	38	-50	86	65 10	50	-2	-82
2101	-13	-34	-14	-18	-52	-34	34	18		2579	20	-18	-70	50	12	12	52	60 0C
2179	-40	-88	20		20	-52				2091	-38	70	48	-52	-12		40	-90
2203	-1	-40	-44	04	-40	-10	44	84		2593	14	-70	98	-14	11	-40		34 cc
2207	40	-40	24 59	-00	90	-34	- 30 - 6	20		2009	-30	-42	-10	50 70	10	0	90 54	00 96
2210	1 4	10	-00	50	-01	50	50	<u>3</u> 0 		2017	10	-04 26	00	-70	0 79	10	-04	20 49
2221	70	-10	-10	-30		49	20	42		2021	22	30 6	-90	-90	-70	-10	50	-42
2231	70	-10	80	19	64	42	30	-42		2033 2647	39	56	-0	42 28	-21	74	-34	-70
2203	-56	-20	28	36	-04	-40	_12	-36		2657	38	18	82	-62	-45 97	18	2	-30
2251	-48	92	-52	-16	-61	-16	-20	-12		2659	40	14	-12	-02	-22	-4	-60	-20
2267	03	18	1	_18	-51	-6	_20	8/		2663	30	24	-16	8/	96	6	8	$\frac{20}{24}$
2269	25	2	62	46	20	50	-34	-2		2671	72	8	-16	8	-64	-28	32	$\frac{21}{24}$
2273	4	18	82	66	42	90	-6	66		2677	-7	32	38	22	-22	50	70	-58
2281	7	-22	-22	58	59	86	-70	-22		2683	-16	20	84	-24	-7	38	-4	4
2287	38	20	72	56	-16	$\begin{vmatrix} 0 \\ 2 \end{vmatrix}$	16	72		2687	23	-12	-72	32	6	42	-48	-48
2293	29	-82	-26	6	80	2	-74	22		2689	5	62	66	98	-46	-10	34	-62
2297	-57	-42	10	90	-27	42	-22	-54		2693	-41	-48	-58	-82	-54	42	-66	-98
2309	60	-12	-0	30	54	-54	30	78		2699	-55	60	-52	-4	0	-36	36	-12
2311	-13	-64	72	8	-64	20	-8	-48		2707	-17	-10	-100	36	-55	50	-28	60
2333	59	-30	62	78	6	18	-34	-26		2711	87	24	8	0	-30	36	80	72
2339	10	-72	-60	24	24	12	28	-20		2713	-56	-94	26	10	-22	-46	58	58
2341	67	20	38	-2	2	-70	-74	-42		2719	-70	-52	80	64	20	8	16	24
2347	-37	80	-44	-52	26	-46	28	52		2729	30	-42	-54	74	-42	-6	18	-6
2351	-48	-24	0	36	-72	-36	48	0		2731	-68	-4	-20	32	50	32	12	-28
2357	-57	-24	-74	-66	9	18	-34	-34		2741	-58	66	54	-26	66	-54	-42	46

					N								Ν	V			
p	11	14	15	17	19	20	21	24	p	11	14	15	17	19	20	21	24
2749	50	-40	-98	70	-76	50	-34	62	3187	-2	-16	-100	12	2	2	-108	-52
2753	49	-78	18	-14	87	90	-94	18	3191	-8	24	8	60	-102	108	-88	56
2767	48	32	40	0	-40	-22	-80	40	3203	-6	24	-36	24	-99	54	-36	28
2777	-42	-18	10	10	-78	18	-78	-22	3209	-10	30	10	58	39	-66	18	-6
2789	-20	60	-26	-26	48	90	30	46	3217	23	86	50	-62	95	50	18	82
2791	42	92	40	28	-43	20	-8	64	3221	-103	-18	-42	6	30	42	38	-18
2797	-42	62	62	-82	-19	-70	-18	-2	3229	70	-46	-2	110	8	98	-2	14
2801	52	30	-14	-30	66	18	50	66	3251	-48	-90	36	4	-72	24	-28	60
2803	44	86	-84	-36	14	38	-76	-100	3253	74	32	-58	62	77	50	-26	38
2819	-25	-66	36	-96	21	-60	84	12	3257	58	30	42	10	-18	18	-6	90
2833	-6	26	18	-78	8	-46	50	-46	3259	-60	56	12	-40	2	20	76	20
2837	-62	42	-42	-42	-93	18	86	46	3271	-3	-40	40	68	-4	-4	40	-32
2843	4	0	20	44	18	-18	-28	-76	3299	100	72	-60	-60	-12	-108	-20	-100
2851	2	44	36	-16	-19	32	52	76	3301	-73	-82	38	-98	44	38	-58	70
2857	-82	-22	-22	-22	50	-46	-54	42	3307	98	14	52	-28	68	-46	108	4
2861	-63	12	14	-42	-90	-66	6	22	3313	4	2	-46	-14	-43	-46	18	-14
2879	-40	-24	64	-68	-96	96	-24	0	3319	0	80	-56	8	-28	8	-24	64
2887	-57	44	-32	28	-28	2	-88	32	3323	-76	-66	-44	-44	108	-114	-36	4
2897	38	54	-30	18	-78	-30	90	-30	3329	-100	-66	-94	66	-6	66	-14	50
2903	54	0	-32	-24	18	6	72	-40	3331	-43	110	-60	-92	65	-88	100	-4
2909	-25	18	-98	-50	72	-30	-66	-10	3343	44	-40	88	76	14	86	-16	104
2917	88	56	-74	-50	2	2	70	-58	3347	-17	36	-36	-4	78	90	76	-20
2927	-72	-96	-24	84	-15	-6	8	-16	3359	-45	-96	96	-20	6	72	80	80
2939	-50	6	-4	-92	18	60	-100	-76	3361	-88	-58	34	-30	86	-34	-30	-30
2953	-86	38	-22	58	-52	74	74	10	3371	-103	-24	-36	72	96	0	-12	-12
2957	3	-96	-82	14	24	-102	-42	-10	3373	4	-28	-34	-58	-10	-46	-98	-66
2963	-81	24	-20	-96	102	-18	28	28	3389	15	42	-34	54	-3	-90	62	22
2969	70	-54	90	10	-93	-66	-54	-6	3391	92	80	-96	8	8	-28	32	-40
2971	-53	38	-4	-20	-61	-88	-36	-12	3407	18	72	-24	-100	0	18	112	-64
2999	-80	36	56	84	45	-24	-24	88	3413	9	-18	86	-74	48	-102	-26	14
3001	27	-58	58	-86	50	-70	42	-38	3433	-66	86	-86	90	-58	26	26	-54
3011	62	24	-44	-84	-27	-48	-36	60	3449	40	-102	58	-38	24	30	66	-102
3019	85	-40	28	80	23	44	12	-28	3457	-57	-34	34	2	56	-70	18	34
3023	39	0	56	84	6	-66	16	64	3461	-38	48	102	-18	12	-42	14	14
3037	13	-40	78	86	95	-22	-34	62	3463	-96	-100	112	44	-1	-82	-56	-16
3041	42	78	-62	-78	-9	30	-102	-14	3467	38	96	116	-52	-12	18	-60	-60
3049	-40	-10	-22	-102	17	26	10	-22	3469	-85	50	-82	30	-49	-10	14	-98
3061	37	-70	-10	70	-34	74	-10	-10	3491	17	102	84	104	24	72	36	-20
3067	13	-64	68	-64	-64	2	-36	20	3499	100	98	28	56	26	68	-100	52
3079	-20	-52	56	0	-7	-64	-40	-80	3511	12	-16	24	96	-52	68	56	0
3083	29	30	-28	96	-24	-42	-68	36	3517	-22	80	-82	-18	-28	2	-2	-98
3089	25	-66	-14	18	57	-30	34	50	3527	18	72	32	-80	-54	18	-104	-88
3109	80	-22	70	-26	-4	-22	-90	70	3529	-35	74	10	-38	-34	-22	-54	74
3119	-90	-96	-48	-104	-6	-72	104	0	3533	24	108	78	-42	24	90	6	118
3121	22	98	50	-14	-109	2	-30	-14	3539	20	36	-44	-16	9	12	44	-36
3137	8	6	-14	-62	102	-102	98	-30	3541	42	-4	22	78	77	-22	86	-74
3163	-26	-22	-76	-4	-13	14	92	-28	3547	53	-34	36	-16	-70	-94	-52	36
3167	18	60	24	52	66	66	96	16	3557	-27	-42	38	70	42	42	-42	-50
3169	45	-34	-30	34	92	50	-62	34	3559	0	-76	-72	-12	41	8	72	0
3181	32	-40	46	14	-94	50	94	-66	3571	-28	-64	-12	-44	80	-88	-12	60

		N											Λ	T			
p	11	14	15	17	19	20	21	24	p	11	14	15	17	19	20	21	24
3581	32	-30	30	86	66	-66	-66	-26	4001	102	-78	-30	2	51	-30	2	2
3583	-96	-88	-88	-16	101	-106	32	-56	4003	-46	-46	28	60	80	-34	-76	-100
3593	-26	42	-38	58	-54	-6	42	-6	4007	-32	72	-32	76	-99	114	8	-40
3607	58	8	112	-84	-55	-118	-88	-64	4013	54	-78	110	-66	-78	42	78	54
3613	-26	-58	46	-34	68	50	62	30	4019	15	60	-76	-24	-18	-12	108	44
3617	63	-42	-46	34	-18	42	106	114	4021	22	44	-74	102	-10	-10	-26	-26
3623	4	-96	-16	0	-54	-18	-112	104	4027	28	-112	36	4	-4	50	-52	52
3631	32	104	-80	-36	14	-76	80	-24	4049	25	-30	50	-14	6	66	90	-46
3637	-72	2	-26	-74	38	98	22	38	4051	-123	38	-76	32	-25	56	-28	-100
3643	34	-10	116	-72	-118	-34	44	-28	4057	103	-10	58	-22	-100	26	-38	90
3659	30	90	12	92	-75	60	12	-60	4073	-31	6	26	122	87	66	82	26
3671	-78	-120	8	24	93	12	40	-72	4079	-60	24	-48	-48	-12	-48	16	-80
3673	-76	74	58	-38	29	50	-70	-38	4091	92	-42	-84	-48	-45	-24	-52	-60
3677	-62	-18	-2	6	72	18	-114	102	4093	94	80	46	-98	116	26	-50	-50
3691	92	-52	-52	20	-7	-88	-20	-92	4099	20	-4	52	76	-94	44	-12	-4
3697	23	-46	-78	-62	-82	-46	50	-14	4111	62	-64	-80	20	80	20	-48	-8
3701	102	-12	54	14	-30	42	-114	30	4127	48	-24	56	-112	81	-54	-88	0
3709	20	-16	-34	6	-70	98	62	-2	4129	-25	-82	98	34	-91	-10	34	34
3719	-55	24	-24	-40	-108	-72	80	-72	4133	4	108	6	102	60	66	-18	-66
3727	23	-88	8	32	-52	98	0	-24	4139	20	-60	12	36	-21	-60	36	116
3733	114	-46	102	-2	-82	-94	54	70	4153	-36	86	26	74	-13	50	-6	-70
3739	-60	-40	76	-100	-112	-76	44	100	4157	-42	72	126	-2	-42	-30	54	54
3761	-88	-42	18	-94	-18	30	18	-110	4159	85	56	-48	-100	-43	56	96	104
3767	-27	96	-48	-12	93	-102	-112	-56	4177	88	74	50	18	-25	2	98	18
3769	40	-10	-70	-86	17	-34	-70	58	4201	-98	-10	-22	26	-28	-22	10	42
3779	-30	54	4	-16	-21	36	-60	-36	4211	-63	-84	-60	32	-72	-72	-4	28
3793	34	-58	-78	-94	-22	-22	34	-14	4217	- 33	-6	42	42	6	-30	-30	-6
3797	-82	-12	-74	-66	42	18	78	94	4219	10	62	44	8	89	-76	28	36
3803	74	-108	20	-8	-78	-18	-44	36	4229	-55	-126	-90	-10	-45	30	-90	-114
3821	-3	96	-50	-114	84	30	118	22	4231	-68	-52	40	0	-34	-28	-40	112
3823	84	-64	-40	104	89	-10	-64	56	4241	92	30	-78	-46	78	30	-6	34
3833	19	42	-54	-86	42	-54	-54	-70	4243	64	32	-20	40	104	-106	-76	-52
3847	-42	-40	-64	-52	-112	26	-40	-16	4253	-16	-78	-34	-26	-6	42	94	-10
3851	-73	72	-36	-60	-6	120	20	36	4259	70	-18	36	-36	-18	-36	-60	-52
3853	74	56	-66	-90	-34	-46	62	94	4261	-113	-4	-26	-18	-67	-70	-58	102
3863	54	-24	32	-56	96	-66	-56	24	4271	-53	-48	-32	0	90	60	72	-48
3877	58	44	-10	102	35	-22	-58	102	4273	-41	-46	82	-14	98	-46	34	-14
3881	7	-18	-22	90	-27	-6	34	-6	4283	39	18	-76	92	-18	54	44	36
3889	-70	110	-14	50	110	38	-14	114	4289	-60	90	34	-62	-114	66	10	-30
3907	-22	20	44	32	92	-22	36	-68	4297	-62	-22	-86	74	-58	-22	-22	-54
3911	12	72	56	8	-105	-60	-72	120	4327	-107	-64	-128	80	-28	122	-8	80
3917	-57	-18	-82	102	72	-78	94	-106	4337	-2	78	34	-14	- 33	66	-14	-30
3919	0	32	64	-104	59	-40	-32	-24	4339	55	38	-28	4	-124	20	100	12
3923	54	-66	-52	100	3	54	36	44	4349	-30	114	-66	6	54	18	-66	-90
3929	-60	-90	-6	10	18	42	122	74	4357	-117	-88	86	-2	-7	2	38	-90
3931	107	8	92	12	35	80	-4	-60	4363	-6	44	-28	64	44	-106	92	-12
3943	-96	56	-48	104	-52	-34	120	-64	4373	84	-24	-106	54	-84	18	-66	62
3947	-107	6	52	24	84	18	-68	52	4391	42	48	120	108	-30	-60	112	24
3967	-92	-100	-8	-68	80	122	-64	88	4397	108	42	-18	-90	-12	-30	78	-90
3989	-90	12	-74	30	-114	78	-114	30	4409	-30	-54	-6	-54	9	-66	66	- 90

				Ν	V								Γ	V			
p	11	14	15	17	19	20	21	24	p	11	14	15	17	19	20	21	24
4421	72	126	70	6	114	90	-10	94	4861	-88	20	-130	-50	65	62	78	78
4423	49	-40	48	60	14	86	56	16	4871	72	-60	-104	80	21	12	72	40
4441	42	-58	90	10	68	-118	90	90	4877	93	12	-50	-18	-114	-126	6	-42
4447	83	-16	-8	44	-7	26	112	56	4889	5	126	26	74	-66	78	114	74
4451	102	114	84	64	-33	96	84	124	4903	-126	116	-16	-28	8	-10	88	96
4457	78	-102	90	26	21	-54	-30	42	4909	115	86	-50	30	-94	-94	-50	-98
4463	-66	24	120	24	-93	6	56	-96	4919	30	36	-72	36	48	-48	-40	-56
4481	82	126	-30	2	-57	-114	-78	66	4931	32	-66	-44	-92	-42	24	-108	-100
4483	-106	38	92	-112	-52	-106	84	92	4933	94	56	22	-34	-124	122	54	86
4493	29	48	-18	54	-39	42	-10	54	4937	-42	54	-102	-38	30	114	26	10
4507	-82	-82	-28	- 36	-28	26	-116	-108	4943	-76	-24	120	-64	-36	54	-104	-32
4513	59	-94	-30	34	-112	-22	-62	-30	4951	-48	56	56	40	56	68	-88	128
4517	8	-114	6	-2	78	-54	-74	30	4957	98	-10	-82	-10	-73	-118	-66	-82
4519	5	-16	-40	60	65	128	-40	16	4967	-52	96	-96	28	-36	-54	-128	72
4523	-36	24	-28	44	69	6	84	-44	4969	100	110	-22	-38	38	-34	-54	-86
4547	-12	-36	12	60	-3	-126	12	92	4973	-1	-96	46	-66	-24	42	118	-74
4549	-10	32	-26	46	-94	14	-90	70	4987	28	-70	-60	48	29	-22	-36	84
4561	112	-118	-46	50	107	50	82	18	4993	44	-46	34	66	44	98	2	2
4567	-112	-112	-112	- 36	23	-22	8	-112	4999	40	-40	-8	-56	-4	56	120	-96
4583	-36	-12	-48	-124	-93	6	8	88	5003	119	-42	36	-24	120	6	-4	-124
4591	-8	-52	112	-80	56	44	-16	-40	5009	-45	-114	114	114	-30	-78	-78	66
4597	-52	-28	-58	-98	134	98	54	118	5011	-38	-118	116	-92	62	80	20	-116
4603	89	-4	-12	108	-76	62	12	-60	5021	-3	102	-2	-10	69	78	78	-42
4621	122	-22	-50	-42	-85	-82	46	46	5023	54	-16	-88	136	-61	-106	-64	-24
4637	18	-108	94	-2	-33	114	-42	38	5039	15	0	48	124	3	-24	48	-48
4639	20	104	80	24	50	-16	32	-56	5051	-48	-36	-116	-60	45	24	68	-44
4643	-81	-24	-36	108	36	-18	-36	44	5059	10	-34	-12	120	-16	116	-60	-20
4649	-80	-30	-54	-38	108	90	-134	-38	5077	8	-70	38	-2	83	26	22	-74
4651	-73	98	-20	-80	80	8	-100	-28	5081	132	114	90	-70	-30	-6	-78	-6
4657	73	50	82	50	86	122	114	50	5087	93	-12	-72	48	18	90	48	0
4663	64	-16	-64	28	-70	-34	88	-64	5099	-10	-78	-116	44	60	-84	-36	36
4673	114	18	82	-46	-24	-54	-30	-78	5101	2	80	46	110	107	-82	62	-34
4679	25	96	-88	24	105	-48	-8	104	5107	-32	68	60	40	-40	26	-76	76
4691	17	-132	36	-12	45	-24	60	12	5113	29	74	-38	-86	92	-70	-102	-6
4703	-36	-84	40	-68	72	126	-16	-64	5119	15	-64	80	-8	44	80	-32	-8
4721	22	66	82	-14	-45	30	-86	-78	5147	48	48	-92	12	-84	138	36	-44
4723	-96	26	44	-16	71	-58	100	44	5153	-111	78	-78	-78	54	-78	-110	114
4729	30	50	122	-86	23	122	-38	-102	5167	28	-16	8	-112	56	-70	112	104
4733	129	18	30	54	-66	-78	-2	38	5171	97	-54	68	-48	-60	120	-60	12
4751	-48	-60	-128	88	81	-84	48	64	5179	-60	-22	-84	16	131	20	76	100
4759	30	116	-56	88	80	-64	56	128	5189	-80	54	6	38	-114	90	86	-82
4783	-101	104	-40	76	-4	110	-96	88	5197	-97	32	126	-42	-4	122	-82	14
4787	8	-54	-36	8	90	-78	100	12	5209	-50	-10	26	10	62	26	90	-38
4789	110	-34	-106	-50	11	110	22	-74	5227	48	98	116	-124	-82	122	-132	-28
4793	-36	-90	-54	-6	-42	42	-94	10	5231	-18	-48	-32	-60	-129	60	24	32
4799	105	-72	0	-44	120	24	56	96	5233	-96	-58	-14	-142	-58	74	114	-14
4801	77	-22	2	-30	-76	-130	-30	66	5237	63	-18	86	-74	36	42	38	30
4813	-76	26	30	46	26	26	46	-50	5261	87	102	46	78	93	78	-98	-42
4817	-132	66	98	-78	-66	90	82	-78	5273	-21	102	42	74	30	-6	90	10
4831	-68	80	-64	-28	8	44	112	-72	5279	-70	24	96	40	-33	-96	-88	16

C Fully Decomposed Prime Numbers

Let E^N denote the modular curve $X_0(N)$. In [Adel94], we single out all fully decomposed prime numbers up to a given bound for certain extensions of \mathbb{Q} constructed by adjoining to \mathbb{Q} the coordinates of *p*-torsion points of E^N . We restrict our attention to those N where E^N is an elliptic modular curve without complex multiplication (see Table A.1) and to *p*-torsion points of orders p = 5, 7, 11. Since our intention is to get numerical data for validation purposes, the bounds limiting our computations are chosen in such way that we expect to find about 20 prime numbers satisfying our conditions. These computations could of course be continued much further.

p	2	3	5	7	11
Degree of $A_p(X)$	3	4	12	24	60
$[\mathbb{Q}(E_p^N):\mathbb{Q}]$	6	48	480	2016	13200
Bound B	_	-	10^{5}	$5 \cdot 10^5$	$3.4 \cdot 10^6$
$\pi(B)$	-	_	9592	41538	243539
Expected Number of Primes	-	_	20	20.6	18.45
Number in $\mathbb{Q}(x(E_p^N))/\mathbb{Q}$	-	_	30 - 43	27 - 42	30 - 49
Number in $\mathbb{Q}(E_p^N)/\mathbb{Q}$	_	_	12 - 25	16 - 23	14 - 23

Table C.1. Data Related to the Computation of Fully Decomposed Prime Numbers

Table C.1 provides an overview of those quantities which limit our computations. $A_p(X)$ is a defining polynomial of the subextension $\mathbb{Q}(x(E_p^N))/\mathbb{Q}$ given by adjunction of the x-coordinates (see Section 3.3 and Section 5.3).

By Proposition 3.5.2, our assumptions above enforce that $\mathbb{Q}(E_p^N)/\mathbb{Q}$ is a Galois extension whose Galois group is isomorphic to $\operatorname{GL}(2,p)$. Its degree is therefore equal to the size of $\operatorname{GL}(2,p)$ which is determined in Proposition 5.1.3. We let $\pi(x)$ denote the number of primes $\leq x$, where x may be any positive real number. The expected number of primes is then calculated

[©] Springer-Verlag Berlin Heidelberg 2001

as the total number of primes below the respective bound divided by the degree of the extension. This value is suggested by the Theorem of Chebotarev (Theorem 2.3.1). The last two rows of Table C.1 show the ranges of the number of fully decomposed primes which are determined in the respective extensions for various curves E^N .

The calculation of fully decomposed prime numbers is performed in two steps:

- Since a particular defining polynomial $A_p(X)$ is known for the subextension $\mathbb{Q}(x(E_p^N))/\mathbb{Q}$, we may take the parameters of the considered curve from Table A.1 and apply Theorem 2.1.1 to them. If ℓ is a prime number to be examined, we have to consider the reduced polynomial $\tilde{A}_p(X) = A_p(X) \mod \ell$ in $\mathbb{F}_{\ell}[X]$. We have to check if $\tilde{A}_p(X)$ splits into distinct linear factors. If this is the case, we may conclude that ℓ is fully decomposed in the subextension $\mathbb{Q}(x(E_p^N))/\mathbb{Q}$. The above condition is satisfied if $\tilde{A}_p(X)$ is a divisor of $X^{\ell} X$ in $\mathbb{F}_{\ell}[X]$. Thus ℓ is fully decomposed in $\mathbb{Q}(x(E_p^N))/\mathbb{Q}$ if and only if we have $X^{\ell} \equiv X \mod \tilde{A}_p(X)$ in $\mathbb{F}_{\ell}[X]$.
- We obtain the relative extension $\mathbb{Q}(E_p^N)/\mathbb{Q}(x(E_p^N))$ by adjoining one y-coordinate of any of the p-torsion points. If ℓ is a prime number which is fully decomposed then ℓ is also fully decomposed in the subextension $\mathbb{Q}(x(E_p^N))/\mathbb{Q}$. Thus $\tilde{A}_p(X)$ necessarily splits over $\mathbb{F}_{\ell}[X]$ into distinct linear factors. We now have to find some zero α of $\tilde{A}_p(X)$. Then we evaluate the Legendre symbol $\left(\frac{f(\alpha)}{\ell}\right)$, where $y^2 = f(x)$ is a defining equation (A.2) of the curve E^N . Thus ℓ is fully decomposed in the p-torsion point extension $\mathbb{Q}(E_p^N)/\mathbb{Q}$ if and only if $\tilde{A}_p(X)$ splits in $\mathbb{F}_{\ell}[X]$ into distinct linear factors and we have $\left(\frac{f(\alpha)}{\ell}\right) = 1$ for some zero α of $\tilde{A}_p(X)$.

All prime numbers ℓ below the bounds given in Table C.1 are checked, and if they satisfy the first or both conditions, they are included in the following tables. The tables are organized as described in Table C.2 below.

Field	$\mathbb{Q}(x(E_5^N))$	$\mathbb{Q}(E_5^N)$	$\mathbb{Q}(x(E_7^N))$	$\mathbb{Q}(E_7^N)$	$\mathbb{Q}(x(E_{11}^N))$	$\mathbb{Q}(E_{11}^N)$
Table	C.3	C.4	C.5	C.6	C.7	C.8

Table C.2. Survey of the Tables of Fully Decomposed Prime Numbers

N	14	15	17	10	00	01	0.4
IN	14	15	17	19	20	21	24
p	1301	5231	2731	2371	2731	2081	3671
	5431	6481	9151	7691	7541	7591	3821
	6761	6491	9221	8011	13681	10531	4721
	15461	7541	12791	8831	18341	14551	13411
	18701	12781	13291	14401	20641	15091	14081
	21601	18451	16451	15331	20731	15401	16301
	24551	22171	23531	15541	22091	16091	16871
	26321	26501	25801	17881	22441	16691	18911
	27031	26891	26591	20431	23561	21871	20731
	29411	28111	26681	21701	32441	22621	30241
	30871	32801	27431	22811	42281	26891	30971
	40231	33211	33581	23801	45191	33811	35111
	43781	39631	34301	26881	48871	37361	36781
	43951	50321	38971	34211	49711	42611	39161
	52021	52501	44071	34511	50891	43271	42821
	52291	57271	45161	35051	56821	44021	43451
	53201	57781	45191	36451	58271	45481	45161
	55051	60161	50321	41161	60091	46171	45691
	56501	61441	58411	49891	60101	50221	45821
	61291	62701	58441	50101	63331	53951	46861
	63131	64081	61961	51061	67141	59221	52301
	70321	73331	62971	54371	69821	61141	53231
	72031	73681	72931	66161	71011	62201	53591
	73681	75181	81901	67511	71741	63691	57781
	75991	75541	82231	72901	72251	67421	58171
	81551	77711	83311	74611	85411	69931	59971
	88651	78401	83891	84391	87491	70991	66071
	92401	87041	88721	84751	88861	71161	66841
	97081	88661	91141	88661	91291	74771	78511
	99251	89261	94111	91151	91331	75941	78791
		89521	95441	91571	94321	76651	82261
		90371	97561	92111	96661	76991	82351
		94331	97841	94261	98011	77291	84131
		99611				77731	84391
		99721				79451	85781
						80831	89501
						87011	90731
						92041	92681
						92551	93911
						96931	95971
						97151	96451
						97501	
						98491	
#	30	35	33	33	33	43	41

Table C.3. Fully Decomposed Prime Numbers in $\mathbb{Q}(x(x))$	$(E_5^N))/\mathbb{Q}$
--	-----------------------

N	14	15	17	19	20	21	24
p	1301	6481	2731	7691	2731	7591	3821
-	15461	12781	12791	8831	22091	14551	4721
	21601	26891	13291	14401	22441	16091	16871
	27031	39631	16451	15541	32441	16691	30241
	43951	52501	27431	26881	45191	22621	35111
	52021	57781	33581	34211	48871	37361	42821
	52291	60161	38971	34511	49711	42611	43451
	53201	62701	44071	35051	58271	45481	45691
	70321	64081	45191	50101	60091	46171	46861
	72031	73331	50321	51061	60101	50221	52301
	75991	73681	72931	54371	67141	59221	53231
	97081	75181	81901	67511	72251	61141	53591
		77711	82231	74611	85411	62201	58171
		78401	83891	84751	87491	63691	59971
		87041	91141	91151	88861	69931	66841
		89261	94111		91291	70991	78511
		89521			91331	71161	78791
		90371			94321	75941	82261
		94331			96661	76991	82351
		99611			98011	77291	84131
		99721				79451	90731
						80831	95971
						96931	
						97501	
						98491	
#	12	21	16	15	20	25	22

Table C.4. Fully Decomposed Prime Numbers in $\mathbb{Q}(E_5^N)/\mathbb{Q}$

N	11	14	15	17	19	20	21	24
p	4831	10487	4733	4691	64891	2087	12041	1583
	17053	28183	35533	42337	66851	22751	13007	7043
	22051	29611	52571	44381	79997	26293	18397	69539
	25033	54293	53201	54979	114269	31963	21841	111539
	36779	70379	55343	78401	125707	36541	25117	122263
	78583	79493	77743	113233	135353	67943	37633	150221
	125441	134597	87403	142157	181273	72227	45613	150893
	129641	162359	92107	146021	211373	81677	90833	153371
	147617	170689	93787	160217	220361	98911	98981	166013
	153287	186481	108109	203911	226913	99149	106121	172999
	173573	191969	113989	226367	240017	101599	107857	193201
	191773	199109	115781	230959	265231	126757	111847	196337
	194027	206081	117839	236909	272777	178487	115837	197597
	195581	211219	124097	270229	283487	197947	131041	210631
	199403	211639	128521	323149	307609	208489	141121	217421
	199501	216679	136193	346039	314651	214607	142031	218107
	201979	230539	146273	352493	320741	224057	232681	260723
	213263	230693	147029	355307	339991	229153	235607	273001
	221159	242887	161323	368089	341041	230273	236461	288359
	243587	249677	163997	393373	356819	236167	236867	292027
	245519	263621	172859	401507	397223	239429	237959	306041
	247381	264391	182617	415577	400331	269221	247591	312509
	260849	281947	190121	417019	408997	300721	281191	319327
	263803	309779	199193	449261	411923	327517	292181	323093
	274121	317773	208699	453377	433847	354551	298327	338171
	304039	368789	210071	456611	438887	370427	321469	341951
	357421	374893	243433	497197	488069	377623	324997	343267
	368117	385589	255977			378127	327559	349553
	374977	404251	269879			399043	337457	354551
	383797	407149	2/1807			415087	339557	355783
	417089	410117	313133			424019	340481	30077
	438047	418027	318179			429731	349483	3/1029
	440715	422479	244177			435239	300277	001709 415577
	470743	424007	044177 200011			445505	266521	415561
	401303	409031	420071			402041	1940121	410001
		476510	430271			407071	404010	424401
		484630	445010			409047	452570	471982
		485647	456/00			492227	467531	486767
		490967	491611			192221	470317	488900
		100001	497491				486949	499927
			499787				100010	100021
#	35	40	42	27	27	39	41	41

Table C.5. Fully Decomposed Prime Numbers in $\mathbb{Q}(x(E_7^N))/\mathbb{Q}$

N	11	14	15	17	19	20	21	24
p	4831	10487	4733	4691	66851	22751	21841	69539
	22051	28183	35533	44381	125707	26293	25117	111539
	78583	54293	77743	54979	135353	67943	37633	166013
	125441	79493	92107	113233	181273	81677	98981	196337
	129641	162359	108109	142157	211373	98911	106121	197597
	147617	206081	113989	146021	220361	126757	115837	210631
	153287	211219	115781	160217	265231	197947	131041	218107
	173573	211639	124097	226367	272777	208489	142031	260723
	195581	230539	128521	236909	307609	229153	232681	273001
	199501	230693	136193	355307	314651	236167	235607	292027
	201979	242887	146273	368089	320741	239429	236461	319327
	221159	263621	147029	415577	339991	300721	236867	323093
	243587	264391	161323	417019	356819	370427	327559	349553
	247381	317773	163997	449261	397223	377623	339557	354551
	274121	385589	210071	453377	400331	399043	340481	355783
	383797	407149	255977	497197	433847	429731	349483	356077
	417089	418027	333019		488069	489847	362741	415661
	438047	422479	344177			490967	434813	424481
	446713	469631	399911				452579	471283
	476743	473789	443129				470317	486767
	481363	476519	456499				486949	499927
		484639	497491					
		490967	499787					
#	21	23	23	16	17	18	21	21

Table	C.6.	Fully	Decomposed	Prime	Numbers	in	$\mathbb{Q}(E_7^N)$)/Q
-------	------	-------	------------	-------	---------	---------------	---------------------	-----

N	11	14	15	17	19	20	21	24
p	109297	141637	168631	16127	18899	67057	176221	72139
	191929	222619	223829	26357	55793	152989	261823	84349
	402029	261031	247853	438527	87517	321311	332641	151537
	486641	312401	373561	552113	94513	395627	572177	202291
	507827	354971	502591	788789	102829	464773	644909	421433
	564367	447701	745933	977087	159347	609313	670781	442201
	797743	488401	764611	996293	253573	687017	692539	613471
	797897	492911	893509	1098439	347359	852457	770837	775633
	838399	509653	956429	1100683	428473	913441	807973	804761
	855031	543929	1142593	1273471	493747	1068761	889043	978209
	866471	579613	1325017	1297297	575257	1129283	909217	1018733
	1037411	589711	1463221	1619773	656063	1152163	1186351	1105193
	1163119	601591	1489753	1709269	718807	1214137	1464079	1161227
	1208681	640949	1593329	1722073	724769	1306889	1582549	1241923
	1536349	678217	1596233	1849849	815431	1541497	1665907	1374847
	1646107	802913	1797049	1881749	997811	1546271	1852819	1563739
	1697191	995347	1810733	1920161	1071907	1557007	1885577	1713823
	1921789	1159027	1907819	1954679	1244629	1697719	1903661	1937123
	1949333	1221463	1920227	2009503	1272151	1733227	2037619	1997293
	1999273	1237897	1972807	2555521	1273757	1958837	2074931	2091431
	2160841	1253803	1978439	2690579	1414381	2247433	2168497	2111803
	2166407	1297451	1998107	2693153	1472791	2293127	2291213	2295481
	2205787	1316261	2028643	2800139	1635173	2315413	2371711	2299463
	2418439	1384351	2048113	2814857	1636867	2376529	2376089	2662903
	2422949	1674949	2149247	2842159	1694023	2411641	2425039	2693263
	2510531	1823999	2264593	2925847	1704979	2438833	2527537	2822909
	2624029	1882519	2359633	2997721	1710677	2488597	2602073	3002231
	2698807	1979891	2528989	3317689	1723481	2491787	2671813	3104641
	2727077	2006093	2668909	3319031	1897787	2499641	2739133	3114563
	2742587	2018897	2721577	3386923	1937123	2505383	2744083	3179551
	2951059	2101199	2746327		2146673	2613953	2822579	3214487
	3235651	2122451	2806211		2167441	2777149	2904287	3283897
		2417339	2846801		2344123	2785157	2928839	
		2435203	2902219		2376331	2880461	2962367	
		2528857	2950223		2434037	2939971	2965777	
		2668051	3142613		2553541	2947429	3115201	
		2770571	3200429		2580689	3049421	3307789	
		2838067			2651419	3077383		
		2838397			2656457			
		2860309			2716319			
		3026783			2846537			
		3123209			2911481			
		3329789			2919577			
		3340679			2978273			
		3353351			2992573			
					3021701			
					3274151			
					3287461			
					3388573			
#	32	45	37	30	49	38	37	32

Table C.7. Fully Decomposed Prime Numbers in $\mathbb{Q}(x(E_{11}^N))/\mathbb{Q}$

N	11	14	15	17	19	20	21	24
p	109297	141637	223829	16127	87517	152989	572177	72139
	402029	261031	247853	26357	94513	609313	644909	202291
	486641	312401	502591	438527	159347	1068761	670781	442201
	507827	447701	893509	552113	815431	1129283	770837	613471
	564367	488401	1142593	996293	997811	1152163	807973	1018733
	797897	492911	1463221	1100683	1414381	1214137	1464079	1105193
	838399	509653	1489753	1273471	1635173	1306889	1582549	1161227
	855031	543929	1596233	1297297	1704979	1541497	1665907	1937123
	1163119	601591	1810733	1881749	1723481	1546271	1885577	1997293
	1208681	1237897	1920227	1954679	1897787	2293127	1903661	2822909
	1536349	1316261	1972807	2555521	2146673	2376529	2037619	3104641
	1646107	1674949	2048113	2693153	2656457	2411641	2074931	3114563
	1949333	1882519	2264593	3317689	2716319	2438833	2168497	3179551
	2160841	2018897	2359633	3319031	2978273	2488597	2291213	3214487
	2205787	2528857	2528989		3274151	2491787	2371711	3283897
	2418439	2668051	2668909		3287461	2505383	2425039	
	2422949	2770571	2721577		3388573	2939971	2527537	
	2727077	2838397	2746327			3049421	2744083	
		2860309	2950223				2822579	
		3026783					2928839	
		3123209					2962367	
		3329789						
		3353351						
#	18	23	19	14	17	18	21	15

Table C.8. Fully Decomposed Prime Numbers in $\mathbb{Q}(E_{11}^N)/\mathbb{Q}$

D Resolvent Polynomials

The images of the elements of the basis $B = \{u_1, u_2, v_2, u_3, u_4, u_6, w_3, w_4, w_5\}$ of $k[x_1, \ldots, x_6]^G$ under the evaluation homomorphism ω are to be determined in Section 6.3, where K is the field $k(x(E_4))$ generated by the x-coordinates of all 4-torsion points of the elliptic curve E and G denotes the realization of the Galois group Gal(K/k) as a subgroup of \mathfrak{S}_6 which is isomorphic to PGL(2, 4). Since the values of the elementary symmetric polynomials in x_1, \ldots, x_6 can be read off from the coefficients of the defining equation, the resolvent polynomials are to be calculated by

$$\mathcal{R}_b(Y) = \omega(\mathcal{RP}_{\mathfrak{S}_6}(b)(Y))$$

for $b \in B$. The coefficients of the last formula, which are symmetric polynomials by Proposition 6.3.3, have to be expressed by the coefficients of the defining polynomial of K/k. The problem reduces to the computation of $\mathcal{R}_b(Y)$ for $b \in \{u_2, u_3, u_4\}$. We finally get

$$\begin{aligned} \mathcal{R}_{u_2}(Y) &= (Y-a) \\ \cdot (Y^6 - 6\,a\,Y^5 + 15\,a^2\,Y^4 - 20\,a^3\,Y^3 - 177\,a^4\,Y^2 - 1296\,a\,b^2\,Y^2 \\ &+ 378\,a^5\,Y + 2592\,a^2\,b^2\,Y - 1215\,a^6 - 15120\,a^3\,b^2 - 46656\,b^4) \\ \cdot (Y^8 - 8\,a\,Y^7 + 28\,a^2\,Y^6 - 184\,a^3\,Y^5 - 864\,b^2\,Y^5 + 326\,a^4\,Y^4 \\ &+ 1728\,a\,b^2\,Y^4 + 200\,a^5\,Y^3 + 1728\,a^2\,b^2\,Y^3 + 7196\,a^6\,Y^2 \\ &+ 103680\,a^3\,b^2\,Y^2 + 373248\,b^4\,Y^2 + 9080\,a^7\,Y + 116640\,a^4\,b^2\,Y \\ &+ 373248\,a\,b^4\,Y + 20225\,a^8 + 274752\,a^5\,b^2 + 933120\,a^2\,b^4) \end{aligned}$$

$$\begin{aligned} \mathcal{R}_{u_3}(Y) &= (Y + 8\,b) \\ \cdot (Y^6 + 48\,b\,Y^5 - 64\,a^3\,Y^4 + 528\,b^2\,Y^4 - 2048\,a^3\,b\,Y^3 - 3584\,b^3\,Y^3 \\ &+ 1024\,a^6\,Y^2 - 8448\,a^3\,b^2\,Y^2 - 42240\,b^4\,Y^2 + 16384\,a^6\,b\,Y \\ &+ 126976\,a^3\,b^3\,Y + 307200\,b^5\,Y - 114688\,a^3\,b^4 - 512000\,b^6) \end{aligned}$$

$$\cdot (Y^8 + 64\,b\,Y^7 + 1792\,b^2\,Y^6 - 1024\,a^3\,b\,Y^5 + 21760\,b^3\,Y^5 \\ &+ 4096\,a^6\,Y^4 + 18944\,a^3\,b^2\,Y^4 + 227968\,b^4\,Y^4 + 65536\,a^6\,b\,Y^3 \\ &+ 376832\,a^3\,b^3\,Y^3 + 1392640\,b^5\,Y^3 + 524288\,a^6\,b^2\,Y^2 + 3604480\,a^3\,b^4\,Y^2 \\ &+ 7782400\,b^6\,Y^2 + 1835008\,a^6\,b^3\,Y + 13238272\,a^3\,b^5\,Y \\ &+ 22528000\,b^7\,Y + 3211264\,a^6\,b^4 + 28672000\,a^3\,b^6 + 64000000\,b^8) \end{aligned}$$

128 D Resolvent Polynomials

$$\begin{aligned} \mathcal{R}_{u_4}(Y) &= (Y+a^2) \\ &\cdot (Y^6 + 6\,a^2\,Y^5 + 15\,a^4\,Y^4 + 20\,a^6\,Y^3 - 177\,a^8\,Y^2 - 2576\,a^5\,b^2\,Y^2 \\ &- 8640\,a^2\,b^4\,Y^2 - 378\,a^{10}\,Y - 5152\,a^7\,b^2\,Y - 17280\,a^4\,b^4\,Y \\ &- 1215\,a^{12} - 32784\,a^9\,b^2 - 342016\,a^6\,b^4 - 1631232\,a^3\,b^6 - 2985984\,b^8\,) \\ &\cdot (Y^8 + 8\,a^2\,Y^7 + 28\,a^4\,Y^6 + 184\,a^6\,Y^5 + 1888\,a^3\,b^2\,Y^5 + 6912\,b^4\,Y^5 \\ &+ 326\,a^8\,Y^4 + 4288\,a^5\,b^2\,Y^4 + 17280\,a^2\,b^4\,Y^4 - 200\,a^{10}\,Y^3 \\ &- 1728\,a^7\,b^2\,Y^3 + 7196\,a^{12}\,Y^2 + 229632\,a^9\,b^2\,Y^2 \\ &+ 2632448\,a^6\,b^4\,Y^2 + 13049856\,a^3\,b^6\,Y^2 + 23887872\,b^8\,Y^2 \\ &- 9080\,a^{14}\,Y - 220064\,a^{11}\,b^2\,Y - 1997056\,a^8\,b^4\,Y \\ &- 8017920\,a^5\,b^6\,Y - 11943936\,a^2\,b^8\,Y + 20225\,a^{16} + 535360\,a^{13}\,b^2 \\ &+ 5313664\,a^{10}\,b^4 + 23445504\,a^7\,b^6 + 38817792\,a^4\,b^8\,) \end{aligned}$$

The representations of the coefficients of the corresponding formal resolvent polynomials $\mathcal{RP}_{\mathfrak{S}_6}(u_i)(Y)$ by elementary symmetric functions in x_1, \ldots, x_6 were computed by programs which were developed within the framework of the dissertation [Adel96]. These polynomials are too large to be given here. For example, the absolute term of $\mathcal{RP}_{\mathfrak{S}_6}(u_4)(Y)$ comprises of 78979 monomials which can be united to 310 orbits under the operation of \mathfrak{S}_6 . A total amount of 283 monomials gives the resulting polynomial expression in the elementary symmetric functions s_j which shrinks under the additional assumption $s_1 = 0$ to 80 monomials.

The substitution of the coefficients of the defining polynomial

$$A(Y) = \frac{1}{2}\Lambda_4(Y) = Y^6 + 5 a Y^4 + 20 b Y^3 - 5 a^2 Y^2 - 4 a b Y - a^3 - 8 b^2$$

and the factorization of the resolvent polynomials obtained this way were performed by Mathematica and verified by MAPLE.

We notice that the list (1, 6, 8) of the degrees of the factors of $\mathcal{R}_{u_i}(Y)$ which are irreducible over k[Y] corresponds bijectively by Theorem 6.3.4 to the list of the orbit lengths of the operation of G on the conjugates of u_i .

From the given information, we conclude by Proposition 6.3.8 that $\mathcal{R}_{u_i}(Y)$ has a single non-repeated linear factor. Since the values of u_i under ω are zeroes of the respective resolvent polynomial, they can be read off from the linear factor of the corresponding resolvent polynomial. The result is

$$\omega(u_2) = a$$
, $\omega(u_3) = -8b$, $\omega(u_4) = -a^2$.

The form of the resolvent polynomials given above can be simplified by suitable substitutions which change the linear factors into the factor Y. The extension of the base field to $k(\mu_4) = k(i)$ leads to a decomposition of the factors of degree 8 into two corresponding factors of degree 4. Using the notations

$$D = -8(4a^3 + 27b^2), \quad C_1 = a^3 + 9b^2, \quad C_2 = 3a^3 + 20b^2, \quad C_3 = -(a^3 + 8b^2),$$

the resolvent polynomials may be written as

$$\begin{aligned} \mathcal{R}_{u_2}(Y) &= Y \cdot (Y^6 + 6 \, a \, D \, Y^2 - D^2) \\ &\cdot (Y^4 + 2(1+i) \, D \, Y + 6 \, a \, D) \\ &\cdot (Y^4 + 2(1-i) \, D \, Y + 6 \, a \, D) \end{aligned}$$
$$\begin{aligned} \mathcal{R}_{u_3}(Y) &= Y \cdot (Y^6 + 2 \, D \, Y^4 - 32 \, C_1 \, D \, Y^2 - 64 \, b^2 \, D^2) \\ &\cdot (Y^4 - 2i \, D \, Y^2 + 16(1+i) \, b \, D \, Y - 72 \, b^2 \, D) \\ &\cdot (Y^4 + 2i \, D \, Y^2 + 16(1-i) \, b \, D \, Y - 72 \, b^2 \, D) \end{aligned}$$
$$\begin{aligned} \mathcal{R}_{u_4}(Y) &= Y \cdot (Y^6 + 2 \, a^2 \, C_2 \, D \, Y^2 - C_3^2 \, D^2) \\ &\cdot (Y^4 + 2(1+i) \, C_3 \, D \, Y + 2 \, a^2 \, C_2 \, D) \\ &\cdot (Y^4 + 2(1-i) \, C_3 \, D \, Y + 2 \, a^2 \, C_2 \, D) \end{aligned}$$

E Free Resolution of the Invariant Algebra

Let k be an algebraic number field and $M = k[x_1, \ldots, x_6]^G$ the algebra of G-invariants where G is the subgroup of \mathfrak{S}_6 of order 48 generated by the cycles (1, 3, 4, 6, 5, 2) and (1, 4, 6, 2)(3, 5). Using the results of Section 6.3, the set $\{u_1, u_2, v_2, u_3, u_4, u_6, w_3, w_4, w_5\}$ is a system of fundamental invariants of M where the indices give rise to the degrees of the respective invariants.

Based on the polynomial algebra $A = k[U_1, U_2, V_2, U_3, U_4, U_6, W_3, W_4, W_5]$ in which the degrees of the generators are suggested by the indices, we get the following free resolution of M as a graded A-module of length 3,

$$0 \to AR_1 \to \bigoplus_{i=1}^5 AQ_i \to \bigoplus_{i=1}^5 AP_i \to A \to M \to 0$$

where P_i , Q_i and R_1 are the homogenous polynomials over A given below. If we write the free resolution in the form $0 \to B_s \to \ldots \to B_0 \to M \to 0$, we get by Hilbert's syzygy theorem (see [Bens93, Cor. 4.2.3])

$$\Phi_M(z) = \sum_{i=0}^s (-1)^i \Phi_{B_i}(z).$$

In our situation we determine the degrees of the polynomials P_i , Q_i and R_1 from the Hilbert-series of M. We get (cf. (6.5))

$$\Phi_M(z) = \frac{1 - z^7 - 2z^8 - z^9 - z^{10} + z^{11} + z^{12} + 2z^{13} + z^{14} - z^{21}}{(1 - z)(1 - z^2)^2(1 - z^3)^2(1 - z^4)^2(1 - z^5)(1 - z^6)}.$$

The set of polynomials $\{P_1, \ldots, P_5\}$ forms a basis of the syzygy ideal of Min A. Consequently, it generates the kernel of the module homomorphism $A \to M$ given by $U_i \mapsto u_i$, $V_i \mapsto v_i$, $W_i \mapsto w_i$. The elements of the module basis $\{1, w_3, w_3^2, w_3^3, w_4, w_5\}$ of M over $k[u_1, u_2, v_2, u_3, u_4, u_6]$ are algebraically dependent, and their products provide the independent syzygies

C. Adelmann: LNM 1761, pp. 131–133, 2001.

[©] Springer-Verlag Berlin Heidelberg 2001

132 E Free Resolution of the Invariant Algebra

$$3w_3w_4 = u_1u_2^2v_2 - u_1^2u_2w_3 + u_1^3u_4 + u_1w_3^2 - 4u_1v_2u_4 + 2u_1u_2w_4 - 3u_2^2u_3 - u_1^2w_5 + 3v_2w_5 + 9u_3u_4$$

$$3w_3w_5 = u_2^3v_2 - u_1u_2^2w_3 + u_1^2u_2u_4 + u_2w_3^2 - u_2^2w_4 - 4u_2v_2u_4 + 2u_1u_2w_5 - 3u_1^2u_6 + 3u_4w_4 + 9v_2u_6$$

$$3w_4^2 = u_2^2v_2^2 - u_1u_2v_2w_3 + u_1^2v_2u_4 - 3u_2u_3w_3 + v_2w_3^2 - 4v_2^2u_4 + 2u_2v_2w_4 - u_1v_2w_5 + 3u_1u_3u_4 + 9u_3w_5$$

$$9w_4w_5 = 2u_1^2u_2^2w_3 - 2u_1u_2^3v_2 - 2u_1^3u_2u_4 - 5u_1u_2w_3^2 - u_1u_2^2w_4 + 8u_1u_2v_2u_4 + 3u_2^3u_3 - u_1^2u_2w_5 + 3u_1^3u_6 + 3u_2^2v_2w_3 + 3u_1^2w_3u_4 + 3w_3^3 - 12v_2w_3u_4 + 6u_1u_4w_4 + 6u_2v_2w_5 - 18u_2u_3u_4 - 18u_1v_2u_6 + 81u_3u_6$$

$$3w_5^2 = u_2^2 v_2 u_4 - u_1 u_2 w_3 u_4 + u_1^2 u_4^2 + w_3^2 u_4 - 4 v_2 u_4^2 - u_2 u_4 w_4 + 2 u_1 u_4 w_5 - 3 u_1 w_3 u_6 + 3 u_2 v_2 u_6 + 9 w_4 u_6$$

We get the homogenous polynomials P_1, P_2, P_3, P_4, P_5 of respective degrees 7,8,8,9,10 by first replacing the invariants by their corresponding indeterminates and then bringing all terms on one side of the equation:

$$P_{1} = U_{1}U_{2}^{2}V_{2} - \ldots + 9U_{3}U_{4} - 3W_{3}W_{4}$$

$$\vdots$$

$$P_{5} = U_{2}^{2}V_{2}U_{4} - \ldots + 9W_{4}U_{6} - 3W_{5}^{2}$$
(E.1)

 Q_1, Q_2, Q_3, Q_4, Q_5 are homogenous polynomials with coefficients from A of respective degrees 11,12,13,13,14 in the indeterminates P_1, \ldots, P_5 to which we assign the respective degrees 7,8,8,9,10 like above. They form a basis for the ideal of syzygies of second kind, i. e. they generate all algebraic dependencies between the P_i . In the current situation, we get Q_1, \ldots, Q_5 from the left hand side of the following identities.

$$(U_1^2 U_2 - 3U_1 W_3 + 6U_2 V_2 - 9W_4) P_1 + (U_1^3 - 6U_1 V_2 + 27U_3) P_2 + (9W_3 - 6U_1 U_2) P_3 + (U_1^2 - 3V_2) P_4 = 0$$

$$(U_1 U_4 - U_2 W_3 + 3W_5) P_1 + (U_1 W_3 - U_2 V_2 - 3W_4) P_2 + (U_2^2 - 3U_4) P_3 + (3V_2 - U_1^2) P_5 = 0$$

$$(6U_2 U_4 - U_2^3 - 27U_6) P_1 + (3U_2 W_3 - U_1 U_2^2 - 6U_1 U_4 + 9W_5) P_2 + (3U_4 - U_2^2) P_4 + (6U_1 U_2 - 9W_3) P_5 = 0$$

$$(U_1^2 U_4 - 2U_1 U_2 W_3 + 3U_1 W_5 + U_2^2 V_2 + 3U_2 W_4 - 12V_2 U_4 + 3W_3^2) P_1 + (U_1 U_2^2 + 6U_1 U_2 - 2U_1 W_2 - 9W_3) P_5 = 0$$

$$+ (U_1U_2^2 + 6U_1U_4 - 3U_2W_3 - 9W_5) P_3 + (U_2V_2 - U_1W_3 + 3W_4) P_4 + (6U_1V_2 - U_1^3 - 27U_3) P_5 = 0$$

$$\left(2U_1U_2W_3 - U_1^2U_4 - 3U_1W_5 - U_2^2V_2 - 3U_2W_4 + 12V_2U_4 - 3W_3^2\right)P_2$$

+
$$(U_2^3 - 6U_2U_4 + 27U_6)P_3 + (U_2W_3 - U_1U_4 - 3W_5)P_4$$

+ $(3U_1W_3 - U_1^2U_2 - 6U_2V_2 + 9W_4)P_5 = 0$

The ideal of syzygies of third kind is generated by a single polynomial R_1 with coefficients from A in the indeterminates Q_1, \ldots, Q_5 of respective degrees 11,12,13,13,14 which has to be homogenous of degree 21 due to the form of $\Phi_M(z)$ given above. R_1 can be read off from the left hand side of the following identity.

$$P_5Q_1 + P_4Q_2 + P_3Q_3 + P_2Q_4 + P_1Q_5 = 0.$$

In this equation, we view the P_i as coefficients from A. The P_i have therefore to be replaced by the expressions indicated in (E.1). We notice that the polynomials P_i appear at two different places of the free resolution.

References

- [Adel94] ADELMANN, CLEMENS : Bestimmung voll zerlegter Primzahlen in Torsionspunkt-Erweiterungen, Research Report, Braunschweig, 1994.
- [Adel96] ADELMANN, CLEMENS : Algebraische und zahlentheoretische Methoden bei der Untersuchung des Zerlegungsverhaltens von Primzahlen in Torsionspunktkörpern elliptischer Kurven, Doctoral Dissertation, Braunschweig, 1996.
- [AtLe70] ATKIN, A. O. L.; LEHNER, J. : Hecke operators on $\Gamma_0(m)$, Mathematische Annalen, vol. 185, 1970, pp. 134-160.
- [Bens93] BENSON, D. J. : Polynomial Invariants of Finite Groups, London Mathematical Society Lecture Note Series 190, Cambridge University Press, Cambridge, 1993.
- [Berl70] BERLEKAMP, E. R. : Factoring Polynomials Over Large Finite Fields, Mathematics of Computation, vol. 24, 1970, pp. 713-735.
- [Bir67] BIRCH, B. J. : Cyclotomic Fields and Kummer Extensions, in: [CaFr67].
- [CaFr67] CASSELS, J. W. S.; FRÖHLICH, A. : Algebraic Number Theory, Academic Press, London, 1967.
- [Cohe93] COHEN, HENRI : A Course in Computational Algebraic Number Theory, Springer, Berlin, 1993.
- [Cox89] Cox, DAVID A. : Primes of the Form $x^2 + ny^2$, Wiley, New York, 1989.
- [Dehn60] DEHN, EDGAR : *Algebraic Equations*, Dover Publications, New York, 1960.
- [Eich54] EICHLER, MARTIN : Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktionen, Archiv der Mathematik, vol. 5, 1954, pp. 355-366.
- [Froh77] FRÖHLICH, A. : Algebraic Number Fields, Academic Press, London, 1977.
- [Gant86] GANTMACHER, FELIX R. : Matrizentheorie, Springer, Berlin, 1986.
- [Gold71] GOLDSTEIN, LARRY JOEL : Analytic Number Theory, Prentice-Hall, Englewood Cliffs, New Jersey, 1971.
- [Hart77] HARTSHORNE, ROBIN : Algebraic Geometry, Springer, New York, 1977.
- [Hass65] HASSE, HELMUT : Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II: Reziprozitätsgesetz, Physica-Verlag, Würzburg, 1965.
- [Hass67] HASSE, HELMUT : Vorlesungen über Klassenkörpertheorie, Physica-Verlag, Würzburg, 1967.
- [Hupp67] HUPPERT, BERTRAM : Endliche Gruppen I, Springer, Berlin, 1967.
- [Ito82] ITO, HIDEJI : A remark on a theorem of Chowla-Cowles, Journal f
 ür reine und angewandte Mathematik, vol. 332, pp. 151-155.
- [Janu73] JANUSZ, GERALD J. : *Algebraic Number Fields*, Academic Press, New York, 1973.
- [Knap92] KNAPP, ANTHONY W. : *Elliptic Curves*, Princeton University Press, Princeton, 1992.
- [Lang76] LANG, SERGE : Introduction to Modular Forms, Springer, Berlin, 1976.

- [Lang78] LANG, SERGE : Elliptic Curves, Diophantine Analysis, Springer, Berlin, 1978.
- [LaTr76] LANG, SERGE; TROTTER, HALE : Frobenius Distributions in GL₂-Extensions, Lecture Notes in Mathematics 504, Springer, Berlin, 1976.
- [Ligo75] LIGOZAT, GÉRARD : Courbes modulaires de genre 1, Bull. Soc. Math. France Mémoires, vol. 43, 1975, pp. 1-80.
- [Macd79] MACDONALD, IAN GRANT : Symmetric functions and Hall polynomials, Clarendon Press, Oxford, 1979.
- [Mazu78] MAZUR, BARRY : Rational isogenies of prime degree, Inventiones mathematicae, vol. 44, 1978, pp. 129-162.
- [McKe94] McKEE, JAMES : Computing Division Polynomials, Mathematics of Computation, vol. 63, 1994, pp. 767-771.
- [Neuk92] NEUKIRCH, JÜRGEN : Algebraische Zahlentheorie, Springer, Berlin, 1992.
- [Rath88] RATHMANN, BRIGITTE : Die Galoisoperation auf Torsionspunkten elliptischer Kurven über Zahlkörpern, Diploma Thesis, Göttingen, 1988.
- [Renn89] RENNEBARTH, NILS : Beispiele von Zerlegungsgesetzen für Torsionspunktkörper elliptischer Kurven, Diploma Thesis, Göttingen, 1989.
- [Serr68] SERRE, JEAN-PIERRE : Abelian l-adic representations and elliptic curves, Benjamin, New York, 1968.
- [Serr72] SERRE, JEAN-PIERRE : Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inventiones mathematicae, vol. 15, 1972, pp. 259-331.
- [Serr73] SERRE, JEAN-PIERRE : A Course in Arithmetic, Springer, New York, 1973.
- [Serr77] SERRE, JEAN-PIERRE : Modular forms of weight one and Galois representations, in: [Froh77], pp. 193-268.
- [Shim58] SHIMURA, GORO : Correspondances modulaires et les fonctions ζ de courbes algébriques, Journal of the Mathematical Society of Japan, vol. 10, 1958, pp. 1-28.
- [Shim66] SHIMURA, GORO : A reciprocity law in non-solvable extensions, Journal für reine und angewandte Mathematik, vol. 221, 1966, pp. 209-220.
- [Shim71] SHIMURA, GORO : Introduction to the Arithmetic Theory of Automorphic Functions, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, 1971.
- [Silv86] SILVERMAN, JOSEPH H. : The Arithmetic of Elliptic Curves, Springer, New York, 1986.
- [Silv94] SILVERMAN, JOSEPH H. : Advanced Topics in the Arithmetic of Elliptic Curves, Springer, New York, 1994.
- [Smi95] SMITH, LARRY: Polynomial invariants of finite groups, A. K. Peters, Wellesley, MA, 1995.
- [Stu93] STURMFELS, BERND : Algorithms in Invariant Theory, Springer, Wien, 1993.
- [SwBi75] SWINNERTON-DYER, H. P. F.; BIRCH, B. J. : Elliptic Curves and Modular Functions, in : BIRCH, B. J.; KUYK, WILLEM : Modular Functions of One Variable IV, Lecture Notes in Mathematics 476, Springer, Berlin, 1975.
- [Tra76] TRAGER, BARRY M. : Algebraic Factoring and Rational Function Integration, Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation, pp. 219-226.
- [Web08] WEBER, HEINRICH : Lehrbuch der Algebra, Band III, 1908. (Reprint, Chelsea, New York, 1961.)

Symbols

$\mathcal{O}_k \dots \dots$	ring of integers of the number field $k, 5$
p	prime ideal of k,i. e. prime ideal of \mathcal{O}_k different from $\{0\}, 5$
$\kappa(\mathfrak{p})$	residue field $\mathcal{O}_k/\mathfrak{p}$ of the prime ideal \mathfrak{p} , 5
K/k	finite extension of number fields, 6
$P_{K/k}(\mathfrak{p})\ldots\ldots$	set of prime ideals of K over \mathfrak{p} , 6
[L:K]	degree of the field extension L/K , 6
$f_{K/k}(\mathfrak{P})$	inertial degree of \mathfrak{P} over $k, 6$
$N_{K/k}$	norm map $K \to k, 6$
$e_{K/k}(\mathfrak{P})$	ramification index of \mathfrak{P} over $k, 6$
(G:H)	Index of the subgroup H in the group G , 6
det	determinant, 8
$\operatorname{Tr}_{K/k}$	trace form of the extension K/k , 8
$d_{K/k}$	discriminant of the extension K/k , 8
Dis(P)	discriminant of the polynomial $P, 8$
$\operatorname{Gal}(K/k) \ldots$	Galois group of the extension K/k , 8
$D_{\mathfrak{P}}$	decomposition group of \mathfrak{P} , 8
$I_{\mathfrak{P}}$	inertial group of \mathfrak{P} , 8
K^H	fixed field of the group $H, 8$
$\pi_{\mathfrak{P}}$	Frobenius automorphism of $\kappa(\mathfrak{P}), 8$
$U \setminus G/V \dots$	set of double cosets of G modulo $U, V, 9$
m	modulus, 11
\mathfrak{m}_0	finite part of \mathfrak{m} , 11
\mathfrak{m}_{∞}	infinite part of \mathfrak{m} , 11
$k_{\mathfrak{m},1}$	ray modulo m, 12
N , $N_{k/\mathbb{Q}}$	absolute norm $k \to \mathbb{Q}, 12$
$I_k \dots$	absolute ideal group of k , 12
$\operatorname{Cl}(k)$	class group of k , 12
h_k	class number of k , 12
I_k^S	group of fractional ideals of k prime to S , 13
$\operatorname{Cl}_{\mathfrak{m}}(k)$	ray class group modulo \mathfrak{m} of k , 13
$[]_{\sim}$	equivalence of ideal groups, 14
$\mathfrak{f}(H)$	conductor of the ideal group H , 14
$\left(\frac{L/k}{\mathfrak{B}}\right)$	Artin symbol, 14
$\widetilde{C}(\mathfrak{p})$	Frobenius class of \mathfrak{p} , 14
$\varphi^{\mathfrak{m}}_{K/L}$	Artin map. 15
$\ker \varphi \ \dots \dots \dots$	kernel of the homomorphism φ , 15
f(K/k)	conductor of the extension K/k . 15
H(K/k)	ideal group of the abelian extension K/k . 16
μ_n	group of <i>n</i> -th roots of unity, 17
$\left(\underline{a}\right)$	nower residue symbol 19
$(p)_{n,k}$	power residue Symbol, 15
$\delta_D(\mathfrak{M})$	Dirichlet density of the set \mathfrak{M} , 22

$\delta_n(\mathfrak{M})$	natural density of the set \mathfrak{M} , 22
$\mathfrak{M}(C)$	prime ideals having Frobenius in the class C , 23
$S(K/k) \dots$	set of fully decomposed prime ideals in K/k , 23
$S_1(L/k)$	set of prime ideals of k having a prime ideal factor of inertial
- ())	degree 1 in L , 24
\overline{K}	separable closure of K , 25
<i>E</i>	elliptic curve, 25
$(X:Y:Z)\ldots$	homogenous coordinates, 25
$\mathbb{P}^{n}(K)$	<i>n</i> -dimensional projective space over K , 25
Δ	discriminant of the elliptic curve E , 26
$i \cdot i(E) \dots$	<i>i</i> -invariant of the elliptic curve E , 26
0	zero element of the addition on E. 27
K[E]	affine coordinate ring of $E_{\rm c}$ 28
A_m , B_m , C_m	division polynomials of $E_{\rm c}$ 28
[n]	multiplication $P \mapsto n \cdot P$ on E. 30
E_{m}	set of <i>n</i> -torsion points of <i>E</i> , 30
$K(E_m)$	n-th torsion point field 30
x(P)	<i>x</i> -coordinate of the point P on E , 31
()	operation of $\operatorname{Gal}(\overline{K}/K)$ on E_{π} 31
$\varphi_n \cdots \cdots$	operation induced by φ_n , 31
$\operatorname{GL}(2,n)$	invertible 2 × 2-matrices over $\mathbb{Z}/n\mathbb{Z}$. 31
$T_{\ell}(E)$	ℓ -adic Tate-module 32
$r_{\ell}(\underline{z})$	ℓ -adic representation End $E \to \text{End } T_{\ell}(E)$. 32
$\pi_a: E \to E \dots$	Frobenius endomorphism of E , 33
a_q	number of points on E rational over \mathbb{E}_{2} , 33
<i>Qq</i>	ℓ -adic representation $\operatorname{Gal}(\overline{K}/K) \to \operatorname{Aut}(T_{\ell}(E))$ 33
\tilde{E}	reduction of E modulo \mathfrak{p} . 35
$Z(\tilde{E}/\kappa(\mathfrak{n}) T)$	n -adic zeta function of $E_{-}37$
$L_{\mathbf{n}}(T)$	p -adic factor of the L-series, 38
$L_{F}(x)$	L-series of the elliptic curve E. 38
$\mathcal{L}_{E/k}(0)$	coefficient of the L-series of E. 38
\mathfrak{H}	upper half plane. 41
$GL(2,\mathbb{R})_+$	2×2 -matrices over R with determinant > 0, 41
\mathfrak{H}^*	extended upper half plane. 42
Γ_{t}	stabilizer subgroup of $t \in \mathfrak{H}^*$ with respect to Γ , 42
X_{Γ}	Riemann surface given by Γ , 42
$a(X_{\Gamma})$	genus of $X_{\rm P}$, 43
$\Gamma(N)$	principal congruence subgroup of level N , 44
$\Gamma_0(N)$	a certain congruence subgroup of level N , 44
$X_0(N)$	modular curve of level N , 44
$[\alpha]_{h}$	operator on meromorphic functions, 46
$F_k(\Gamma)$	modular functions of weight kwith respect to Γ . 46
$M_{h}(\Gamma)$.	modular forms of weight k with respect to Γ 46
$S_{k}(\Gamma)$	cusp forms of weight k with respect to Γ 46
$\sim \kappa (1) \cdots \cdots \cdots$	casp forms of worghe is when respect to 1, 10

$G_{2k}(\tau)$	Eisenstein series of weight $2k$, 47
$\Delta(\tau)$	Δ -function, 47
$j(\tau)$	<i>j</i> -function, 47
$R(\Gamma, \Delta) \dots$	Hecke ring, 48
T_n	Hecke operator, 49
$T_n^{(k)}(f)$	Hecke operator on $F_k(\Gamma)$, 49
\mathcal{R}_n	system of representatives for T_n , 49
$Y_0(N)$	modular curve $X_0(N)$ minus its cusps, 49
Λ_{τ}	lattice $\mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau$ in \mathbb{C} , 50
$\langle f, g \rangle_k \dots$	Petersson product of f and g , 52
$L_f(s)$	L-series of the cusp form f , 53
$\mathcal{A}(C_1, C_2) \dots$	group of algebraic correspondences from C_1 to C_2 , 54
K^{t}	transpose of the correspondence K , 54
$\Pi_p \ldots \ldots$	Frobenius correspondence on $\tilde{X}_0(N)$, 55
$\eta(\tau)$	η -function, 57
$Z(G) \ldots \ldots$	center of the group G , 59
SL(2,n)	2×2 -matrices over $\mathbb{Z}/n\mathbb{Z}$ with determinant 1, 59
R_{p^m}	kernel of the reduction map $\operatorname{GL}(2, p^m) \to \operatorname{GL}(2, p^{m-1}), 61$
$\dot{M}(2,n)$	2×2 -matrices over $\mathbb{Z}/n\mathbb{Z}$, 61
$\mathfrak{S}_n \dots \dots$	symmetric group on n symbols, 63
\mathfrak{A}_n	alternating group on n symbols, 63
$\psi(n)$	number of cyclic subgroups of size n of E_n , 64
e_n	Weil pairing $E_n \times E_n \to \mu_n$, 67
J_n , $J_n(E)$	set of <i>j</i> -invariants of the quotient curves $E/U, U \leq E_n$ cyclic
	of size $n, 68$
$\operatorname{Res}_X(P,Q)$	resultant of the polynomials P, Q with respect to $X, 73$
$\Phi_n(X,Y)$	n-th modular polynomial, 74
$\phi_n(X)$	n-th cyclotomic polynomial, 74
$\Lambda_n(X)$	n-th reduced division polynomial, 74
$k_{\Delta,n}$	splitting field of $X^n - \Delta$ over $k, 81$
N_f	set of zeroes of the polynomial f , 87
<i>k</i>	algebraic closure of $k, 87$
k_f	splitting field of the polynomial f , 87
ν	enumeration map, 87
$\operatorname{Stab}_U(P)$	stabilizer of the polynomial P in $U \leq \mathfrak{S}_m$, 88
$k[x_1,\ldots,x_m]^U$	k-algebra of U -invariants, 88
ω_f	evaluation homomorphism $k[x_1, \ldots, x_m] \to k_f, 88$
R_f	ideal of the polynomial relations, 88
$\operatorname{Gal}(f/k) \ldots$	Galois group of the polynomial f over k , 88
r_{ν}	injection of $\operatorname{Gal}(f/k)$ into \mathfrak{S}_m , 89
$\Phi_A(z)$	Hilbert-series of the graded algebra A , 91
$R_U \dots \dots$	Reynolds operator of $U \leq \mathfrak{S}_m, 92$
$\underline{\mathcal{RP}}_{W \leq U} \dots \dots$	formal resolvent polynomial of $W \leq U \leq \mathfrak{S}_m$, 92
$R_U \dots \dots$	modified Reynolds operator, 93

$M(\pi)$	permutation matrix assigned to $\pi \in \mathfrak{S}_m$, 94
$\mathcal{R}_{U,P}$	resolvent polynomial to the polynomial P , 95
E^{N}	modular curve $X_0(N)$, 119
$\pi(x)$	number of primes $\leq x$, 119

Index

Artin map, 15 Artin symbol, 14 averaging operator, 92 card, 42class group, 12 class number, 12 Cohen-Macaulay algebra, 91 complex multiplication, 34 conductor, 14 congruence, 11 congruence subgroup, 44 correspondence - algebraic, 54 - dual, 54 - transposed, 54 cubic resolvent, 77 cusp, 42cusp form, 46 cycle type, 95 cyclotomic extension, 21 cyclotomic polynomial, 74 decomposition field, 8 decomposition group, 8 decomposition law, 6 - of 2-torsion point fields, 78 - of 3-torsion point fields, 79 - of 4-torsion point fields, 83 - of abelian extensions, 17 - of cyclic Kummer extensions, 18 - of cyclotomic extensions, 21 decomposition type, 83 defined modulo m, 13 density - Dirichlet, 22 - natural, 22 discriminant, 8 division polynomials, 28 Eichler-Shimura Formula, 55

elliptic curve, 25

elliptic point, 42 Frobenius automorphism, 8 fully decomposed, 6 fundamental domain, 52 fundamental invariant, 94 genus, 43 graph, 54 Hecke operator, 49 Hecke ring, 48 Hilbert-series, 91 Hironaka decomposition, 91 homogenous set of parameters, 91 homothetic, 49 ideal class group - generalized, 13 ideal group, 14 – absolute, 12 inertial degree, 6 inertial field, 8 inertial group, 8 j-invariant, 26 Krull dimension, 91 Kummer extension, 17 - cyclic, 18 L-series - of a cusp form, 53 - of an elliptic curve, 38 modular curve, 44 modular form, 46 modular function, 46 moduli space, 49 modulus, 11 modulus of definition, 13 multiplicative, 51

orbit, 41 Petersson product, 52 place, 11 - complex, 11 - finite, 11 - infinite, 11 - real, 11 power residue symbol, 19 primary invariant, 94 principal congruence subgroup, 44 ramification index, 6 ramified, 6 ray class extension, 16 ray class group, 13 ray modulo m, 12 reduction - additive, 35 - bad, 35 - good, 35 - multiplicative, 35 -- split, 35 representation - l-adic, 32

residue field, 5 resolvent polynomial, 95 - formal, 92 Reynolds operator, 92 Riemann surface, 42 ring of integers, 5 secondary invariant, 94 semistable, 35 splitting field, 87 syzygy, 102 Tate-module, 32 torsion point, 27 torsion point extension, 30 torsion point field, 30 U-invariant, 88 unramified, 6 Weil pairing, 67 zeta function - p-adic, 37