UNIVERSITÀ DEGLI STUDI ROMA TRE
FACOLTÀ DI SCIENZE MATEMATICHE FISICHE NATURALI

Graduation Thesis in Mathematics
by

Alfonso Pesiri

The Chebotarëv Density Theorem Applications

Supervisor

Prof. Francesco Pappalardi

The Candidate The Supervisor

ACADEMIC YEAR 2006 - 2007
OCTOBER 2007

AMS Classification: primary 11R44; 12F10; secondary 11R45; 12F12.
Key Words: Chebotarëv Density Theorem, Galois theory, Transitive groups.

Contents

Introduction

The problem of solving polynomial equations has interested mathematicians for ages. The Babylonians had methods for solving some quadratic equations in 1600 BC. The ancient Greeks had other methods for solving quadratic equations and their geometric approach also gave them a tool for solving some cubic equations. In AD 1500 a formula for solving cubic equations was found, although it is uncertain who was the first to discover it. About 1515, Scipione del Ferro solved some instances of $x^3 = px + q$, but kept his solution secret. In 1535 Tartaglia rediscovered the solution of $x^3+px = q$. Eventually Tartaglia told his solution to Cardano; he completed the remaining cases and published them in his famous *Ars Magna*, which also contained a method for solving the quartic equation. About 1545, Lodovici Ferrari discovered the quartic formula. Algebraic notations of equations were introduced by Descartes in the 17th century.

n	Polynomial	Zeroes
1	$ax + b,\ a \neq 0$	$x = -\frac{b}{a}$
2	$x^2 + ax + b$	$x = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}$
3	$x^3 + ax^2 + bx + c$	$y_1 = \beta + \gamma,\ y_2 = \beta\zeta_3 + \gamma\zeta_3^2,\ y_3 = \beta\zeta_3^2 + \gamma\zeta_3$ $\beta = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ $\gamma = \sqrt[3]{-\frac{q}{2} \mp \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ $x = y - \frac{a}{3},\ p = \frac{3b-a^2}{3},\ q = \frac{2a^3-9ab+27c}{27}$
4	$x^4 + ax^3 + bx^2 + cx + d$	too long for this presentation

Table 1: Solutions for polynomial equations.

Since it was now possible to solve all polynomial equations of degree ≤ 4 by radicals, the next problem was how to solve the quintic equation. In 1770 Lagrange proved that the tricks used to solve equations of a lower degree do not work for the quintic. This arose the suspicion that the quintic equation may not be always solvable by radicals. The first person to publish a proof for this was Ruffini. He made a first attempt in 1799 in his book *Teoria Generale delle Equazioni* and then tried again with a better, but still not accurate, proof in a journal in 1813. In 1824 Abel filled the gap in Ruffini's proof. Actually, neither the proof of Ruffini nor that of Abel is correct in details, but Abel's proof was accepted by his contemporaries and Ruffini's was not. Kronecker published in 1879 a simpler proof that there is no formula for solving all quintic equations by radicals. This led to a new question: how can we see if a special equation can be solved by radicals? In 1843 Liouville wrote to the Academy of Science in Paris that, among the papers of the late Galois, he had found a proof that the quintic is insoluble by radicals: this was the origin of the Galois theory.

The problem of determining the Galois group of a polynomial from its coefficients has held the interest of mathematicians for over a hundred years. There is a classical algorithm for determining the Galois group of a polynomial from its roots which can be found in Section 2.2, but the method is cumbersome and is not of much interest from a practical point of view. More recently Richard Stauduhar has applied modern insights to old techniques, to develop and implement a computer algorithm that finds Galois groups of low degree polynomials with integer coefficients, as explained in [Sta73]. We will follow a different way, based fundamentally on a technical but powerfull theorem in Algebraic Number Theory: *the Chebotarëv Density Theorem*. This theorem is due to the Russian mathematician Nikolai Grigor'evich Chebotarëv, who made his discovery in 1922, as he recalls in a letter of 1945:

> I belong to the old generation of Soviet scientists, who were shaped by the circumstances of a civil war. I devised my best result while carrying water from the lower part of town (Peresypi in

> Odessa) to the higher part, or buckets of cabbages to the market, which my mother sold to feed the entire family.

To describe Chebotarëv's theorem, let us denote with L/K a finite Galois extension of algebraic number fields with group G. For each prime ideal $\mathfrak{p} \in K$ which is unramified in L, let $\sigma_{\mathfrak{p}}$ denote its *Frobenius element*. Then the Dirichlet density of the set of prime ideals with a given Frobenius element C exists and equals $|C|/|G|$.
The construction of the Frobenius element is mildly technical, which forms the main cause for the relative unpopularity of Chebotarëv's theorem outside Algebraic Number Theory.

In **Chapter 1** we introduce the algebraic knowledges necessary to understand the Frobenius element. We can characterize this element in the abelian case with the following.
Theorem 1.2.1. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial such that $\mathrm{Gal}(f) = \mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})$ is abelian, and p be a prime number not dividing $\Delta(f)$. Then there is a unique element $\varphi_p \in \mathrm{Gal}(f)$ such that the Frobenius map of the ring $\mathbb{F}_p[\alpha]$ is the reduction of φ_p modulo p; this means that, in the ring $\mathbb{Q}[\alpha]$, one has*

$$\alpha^p = \varphi_p(\alpha) + p \cdot (q_0 + q_1\alpha + \cdots + q_{n-1}\alpha^{n-1})$$

for certain rational numbers $q_0, \ldots, q_{n-1}$ of which the denominators are not divisible by p.

We start considering minimal abelian extensions of $K = \mathbb{Q}$. Elementary considerations in the case of a quadratic extension $\mathbb{Q}(\sqrt{D})$, where D is square–free, lead us to a very explicit description of the fact: if we identify $\mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$ with the multiplicative group of two elements $\{\pm 1\}$, then φ_p turns out to be the Legendre symbol $\left(\frac{D}{p}\right)$. Another easy case is the cyclotomic one: in this situation σ_p is the element of $\mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma(\zeta_n) = \zeta_n^p$. In fact, modulo p we have

$$\sigma\left(\sum a_i\zeta_n^i\right) = \sum a_i\zeta_n^{ip} = \sum a_i^p\zeta_n^{ip} = \left(\sum a_i\zeta_n^i\right)^p$$

as required. Therefore, if we identify $\mathrm{Gal}(\Phi_m)$ with $(\mathbb{Z}/m\mathbb{Z})^*$, the Frobenius element of a prime ideal $\mathfrak{p} = p\mathbb{Z}$ is simply given by $p \bmod m$.

Thus the Frobenius element of a prime ideal $\mathfrak{p} \in \mathcal{O}_K$ is always an element of $\mathrm{Gal}(L/K)$, where L is the splitting field of $f(x) \in K[x]$. It's interesting to notice that the degree of each irreducible factor of the polynomial $(f \bmod p)$ in $\mathbb{F}_p[x]$ is equal to the order of φ_p in the group G. In particular, one has $\varphi_p = id$ in G if and only if $(f \bmod p)$ splits into n linear factors in $\mathbb{F}_p[x]$. This will be fundamental in order to relate the Chebotarëv theorem to the computation of Galois groups.

A general discussion on the Frobenius element put us inside the theory of *Dedekind Domains.* The notions of *Decomposition group*

$$G(\mathfrak{P}) := \{\sigma \in G \text{ s.t. } \sigma\mathfrak{P} = \mathfrak{P}\}$$

of a prime ideal $\mathfrak{P} \in \mathcal{O}_L$ s.t. $\mathfrak{P}|\mathfrak{p}$ lead us to the following definition.

Definition 1.6.5. *We define the Frobenius element $\sigma_{\mathfrak{P}} = (\mathfrak{P}, L/K)$ of $\mathfrak{P}$ to be the element of $G(\mathfrak{P})$ that acts as the Frobenius automorphism on the residue field extension $F_{\mathfrak{P}}/F_{\mathfrak{p}}$.*

Even if it's a general characterization, it does not give information about a constructive method for the computation of the Frobenius element.

In **Chapter 2** we explore three theorems which can be regarded as particular case of the main theorem. Finally we state a reformulation of the Chebotarëv Density theorem.

Theorem 2.5.1 *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial. Assume that the discriminant $\Delta(f)$ of $f(x)$ does not vanish. Let C be a conjugacy class of the Galois group $G = \mathrm{Gal}(f)$. Then the set of primes p not dividing $\Delta(f)$ for which σ_p belongs to C has a density, and this density equals $|C|/|G|$.*

Since the cycle pattern of $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(f)$, with $\mathfrak{p} = p\mathbb{Z}$, equals the decomposition type of $f \bmod p$, the above theorem implies the following, sometimes called *Dedekind's Theorem.*

Corollary 2.2.4. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree m,* *and let p be a prime number such that* $(f \bmod p)$ *has simple roots, that is* $p \nmid \Delta(f)$. *Suppose that* $(f \bmod p) = \prod f_i$, *with f_i irreducible of degree m_i in* $\mathbb{F}_p[x]$. *Then* $\mathrm{Gal}(f)$ *contains an element whose cycle decomposition is of type* $m = m_1 + \cdots + m_r$.

The above result give the following strategy for computing the Galois group of an irreducible polynomial $f \in \mathbb{Z}[x]$. Factor f modulo a sequence of primes p not dividing $\Delta(f)$ to determine the cycle types of the elements in $\mathrm{Gal}(f)$; continue until a sequence of prime numbers has yielded no new cycle types for the elements. Then attempt to read off the type of the group from tables of transitive groups of degree ∂f. To make the computation more effective, in a technical sense, we need the *Frobenius Theorem.*

Theorem 2.3.1. *The density of the set of prime p for which $f(x)$ has a given decomposition type $n_1, n_2, \cdots, n_i$, exists, and it is equal to* $1/\#\mathrm{Gal}(f)$ *times the number of $\sigma \in G$ with decomposition in disjoint cycle of the form $c_{n_1} c_{n_2} \cdots c_{n_i}$, where c_{n_k} is a n_k-cycle.*

The Frobenius Density Theorem, which Chebotarëv generalizes, says that if a cycle type occurs in $\mathrm{Gal}(f)$, then this will be seen by looking modulo a set of prime numbers of positive density. To compute $\mathrm{Gal}(f)$, look up a table of transitive subgroups of S_n with order divisible by n and their cycle types distribution. We will see that this strategy is not always effective, and other tools are needed.

The Frobenius Density Theorem is a specialization of the main theorem in which C is required to be a *division* of G rather than a conjugacy class; here we say that two elements of G belong to the same division if the cyclic subgroups that they generate are conjugate in G. The partition of G into divisions is, in general, less fine than its partition into conjugacy classes and Frobenius's theorem is correspondingly weaker than Chebotarëv's.

Last theorem discussed is the celebrated *Dirichlet's Theorem on Primes in Arithmetic Progression.*

Theorem 2.6.1. *For each pair of integers a, m such that* $\gcd(a, m) = 1$, *the set S of prime numbers p such that* $p \equiv a \bmod m$ *has density* $1/\varphi(m)$, *where*

φ is the classical Euler function.

It's an easy consequence of the main theorem, based on the fact that there is a bijective correspondence between the conjugacy classes mod$m$ of prime numbers that do not divide m and the elements of the group $\mathrm{Gal}(\Phi_m)$, which is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$, given by the map $p \leftrightarrow \sigma_p$, so that we may identify σ_p with p mod m, as explained in Chapter 1. Hence

$$\delta\left(p \equiv a \bmod m\right) = \delta\left(p \text{ s.t. } \sigma_p : \zeta_m \mapsto \zeta_m^a\right) = \frac{1}{\varphi(m)}.$$

This chapter ends with an elementary proof of Chebotarëv's theorem in the quadratic case, based on the theory of congruences. Finally is given a more extensive, but not general, proof which follows Chebotarëv's original strategy, avoiding the technical *Class Field Theory*.

Chapter 3 deals with applications of the main theorem. The first one is about polynomials which have a root modulo almost all primes, that is, except for a finite number of primes.

Theorem 3.1.7. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial that has a zero modulo almost all primes p. Then $f(x)$ is linear.*

Next, we have an interesting result about primes p for which f mod p has no zeros.

Theorem 3.1.1. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree $n > 1$. If p is prime, let $N_p(f)$ be the number of zeros of f in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Then there are infinitely many primes p such that $N_p(f) = 0$. Moreover the set $P_0(f)$ of p's with $N_p(f) = 0$ has a density $c_0 = c_0(f) \geq 1/n$.*

The proof is long but not difficult, an is based on Burneside's Lemma. A collateral consequence of this lemma is that the mean value of $N_p(f)$ for $p \to \infty$ is equal to 1. In other words,

$$\sum_{p \leq x} N_p(f) \approx \pi(x) \text{ when } x \to \infty,$$

where $\pi(x) = \#\{p \text{ primes s.t. } p \leq x\}$.

The third argument is a classical theorem about primitive positive definite quadratic forms $ax^2+bxy+cy^2$ which represent prime numbers. We will just consider particular cases, obtaining results of the type

$$\delta(p \geq 3 \text{ s.t. } p = x^2 + ny^2) = \frac{1}{2},$$

for all n such that the class number $h(-4n)$ equals 1.
The rest of the Chapter takes care for illustrate how the Chebotarëv theorem can be combined with other tools in order to get a powerfull algorithm to compute Galois groups of irreducible polynomials in $\mathbb{Z}[x]$. The strategy is as follows.

1. test whether f is irreducible over $\mathbb{Z}$;

2. compute the discriminant $\Delta(f)$;

3. factor f modulo primes not dividing the discriminant until you seem to be getting no new decomposition type;

4. compute the orbit lengths on the r–sets of roots;

5. use tables of transitive groups of degree ∂f.

If $\partial f \leq 7$, then third point suggested by Chebotarëv's theorem is effective, but for higher degrees, this test gets into problems. In fact it is possible to construct two non–isomorphic groups which have transitive permutation representations in which the number of elements with a given cycle structure is the same for both groups. In this situation other tests, like the one suggested at point 4, are relevant.
Point 5 requires the knowledge of transitive permutation groups, so in the last section of the chapter we include tables for groups of degree 3, 4, 5, 6, 7 and 11, as well.

The aim of **Chapter 4** is to analyze the Maple code, given in Appendix C, based on the modulo p reductions test suggested by the Chebotarëv theorem, for polynomials of degree from 3 to 7, and 11.

We tabulate several outputs in order to give an idea of the accuracy of our tests, which depends on the choice of the upper bound k representing the size of prime numbers that we want to consider. If we increase k, on the one hand our result will be more precise, on the other hand Maple will need more time to produce the output.
The polynomials considered are those of the type $f(x) = x^n + 2$ and those in Table 4.1 and 4.2 with Galois group A_n.
Then we introduce a notion of relative error $\epsilon(G) = \epsilon(G,\, k)$ of the test, which measure the *distance* between the theoretical and the empirical result. From the analysis of these errors we notice that

$$\epsilon(G,\, 10^6) < 10^{-2} \text{ and } \epsilon(G,\, 10^3) < 10^{-1},$$

and, by induction, one may naively guess $\epsilon(10^{3t}) < 10^{-t}$, $t \geq 1$, when $G = \mathrm{Gal}(f)$. This observation indicates that $k \geq 10^3$ usually is a good bound for the Chebotarëv test.
This tool allows us to make several experiments in finding polynomial with a given Galois group. In our attempts, we ran the program for all the polynomials in Table 4.1 and 4.2, partially taken from [SM85], in which each transitive permutation group of degree from 3 to 7 and 11 is realised as a Galois group over the rationals. The choice $p \leq k = 1000$ gave always the correct output.

The chapter goes on with a section on the computation of Galois groups for polynomials of prime degree p. We develop an algorithm based on the existence of non–real roots of a polynomial.
If a prime degree polynomial $f(x)$ has $r = 2s$ complex roots, then we know that a permutation of the type $(2)^{\frac{r}{2}}$ is in its Galois group. Hence, the list of possible Galois groups for $f(x)$ is much shorter than in general. Knowledge of r provides us a further information: from a theorem of Jordan, it follows that if r is small enough with respect to the degree p of the polynomial, then the Galois group is A_p or S_p. The specific statement follows as a theorem.
Theorem 4.2.2. *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree $p \geq 3$ and $r = 2s$ be the number of non–real roots of $f(x)$. If s*

satisfies

$$s(slogs + 2logs + 3) \leq p$$

then $\mathrm{Gal}(f) = A_p$, *or* S_p.

If we consider $f(x)$ such that $\partial f = p \leq 29$, no two groups have the same cycle structure, and so the Galois group can be determined uniquely by reduction modulo p for all polynomials of prime degree ≤ 29.
Combining the above results we have an algorithm for computing the Galois group of prime degree polynomials with non–real roots.

```
begin
r:=Number Of Real Roots(f(x));
  if p > N(r) {
    if D(f) is a square {
      Gal(f)=A_p;
    else Gal(f) = S_p;
    }
  else Chebotarev test(f(x));
  }
end;
```

We remark that while the Chebotarëv test is difficult to execute from a computational point of view, checking whether a polynomial has non–real roots is very efficient since numerical methods can be used.

Chapter 1

Algebraic background

1.1 The Frobenius Map

Every field has a unique minimal subfield, the *prime subfield*, and this is isomorphic either to $\mathbb{Q}$ or to $\mathbb{Z}_p$, where p is a prime number. The proof of this fact is easy and can be found in [Rot95]. Correspondingly, we say that the *characteristic* of the field is 0 or p. In a field of characteristic p we have $px = 0$ for every element x, where as usual we write

$$px = (1 + 1 + \cdots + 1)x$$

where there are p summands 1, and p is the smallest positive integer with this property. In a field of characteristic zero, if $nx = 0$ for some non–zero element x and integer n, then $n = 0$.

Theorem 1.1.1. *Let p be a prime number and R be a commutative ring of characteristic p. Then $F : a \mapsto a^p$ is a ring homomorphism from R to itself.*

Proof. Clearly $F(a \cdot b) = (a \cdot b)^p = a^p \cdot b^p = F(a) \cdot F(b)$, for any a, $b \in R$. Then $F(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} \cdot b^k$. Since $p | \binom{p}{k}$, for all $k = 1, 2, \ldots p-1$, we get $F(a + b) = a^p + b^p = F(a) + F(b)$. □

The map in Theorem 1.1.1 is called the *Frobenius Map* after Georg Ferdinand Frobenius, realized its importance in Algebraic Number Theory in

1880.

Now, our goal is answering the following question: which ring homomorphism $R \to R$ is F, that is, does F have a more direct description than through p–th powering? We study two cases in which this can be done. Throughout we let p be a prime number. The simplest ring of characteristic p is the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of integers modulo p. Since any element of $\mathbb{F}_p$ can be written as $1 + 1 + \ldots + 1$, the only ring homomorphism $\mathbb{F}_p \to \mathbb{F}_p$ is the identity. In particular the Frobenius map $F : \mathbb{F}_p \to \mathbb{F}_p$ is the identity. Looking at the definition of F we see that this observation proves *Fermat's Little Theorem*: for any integer a one has $a^p \equiv a \pmod{p}$. Next we consider quadratic extensions of $\mathbb{F}_p$. Let d be a non–zero integer, and let p be a prime number not dividing $2d$. We consider the ring $\mathbb{F}_p[\sqrt{d}]$ the elements of which are by definition the formal expressions $u + v\sqrt{d}$, with u and v ranging over $\mathbb{F}_p$. If d is not a square modulo p, then no two of these expressions are considered equal and, therefore, the number of elements of the ring equals p^2. The ring operations are the obvious ones suggested by the notation, that is, we define

$$\begin{aligned} (u + v\sqrt{d}) + (u' + v'\sqrt{d}) &= (u + u') + (v + v')\sqrt{d}, \\ (u + v\sqrt(d)) \cdot (u' + v'\sqrt{d}) &= (uu' + vv'd) + (uv' + vu')\sqrt{d}, \end{aligned} \qquad (1.1)$$

where d in $vv'd$ is interpreted to be the element $d \pmod{p}$ of $\mathbb{F}_p$. It is straightforward to show that with these operations $\mathbb{F}_p[\sqrt{d}]$ is a ring of characteristic p. Let us now apply the Frobenius map F to a typical element $u + v\sqrt{d}$. Using, in succession, the definition of F, the fact that it is a ring homomorphism, Fermat's little theorem, the defining relation $(\sqrt{d})^2 = d$ and the fact that p is odd, we find

$$F(u + v\sqrt{d}) = (u + v\sqrt{d})^p = u^p + v^p(\sqrt{d})^p = u + vd^{(p-1)/2}(\sqrt{d}).$$

This leads us to investigate the value of $d^{(p-1)/2}$ in $\mathbb{F}_p$. Again, from Fermat's little theorem, we have

$$0 = d^p - d = d \cdot (d^{(p-1)/2} - 1) \cdot (d^{(p-1)/2} + 1).$$

Since $\mathbb{F}_p$ is a field, one of the three factors d, $(d^{(p-1)/2}-1)$, $(d^{(p-1)/2}+1)$ must vanish. As p does not divide d it is exactly one of the last two. The quadratic residue symbol $\left(\frac{d}{p}\right)$ distinguishes the two cases: for $d^{(p-1)/2} = +1$ in $\mathbb{F}_p$ we put $\left(\frac{d}{p}\right) = +1$, and for $d^{(p-1)/2} = -1$ we put $\left(\frac{d}{p}\right) = -1$. The conclusion is that the Frobenius map is one of the two *obvious* automorphisms of $\mathbb{F}_p[\sqrt{d}]$: for $\left(\frac{d}{p}\right) = +1$ it is the identity and for $\left(\frac{d}{p}\right) = -1$ it is the map sending $u+v\sqrt{d}$ to $u-v\sqrt{d}$. The assignment $u+v\sqrt{d} \mapsto u-v\sqrt{d}$ is clearly reminiscent of complex conjugation, and it defines an automorphism in far more general circumstances involving square roots. For example, we may define a ring $\mathbb{Q}[\sqrt{d}]$ by simply replacing $\mathbb{F}_p$ with the field $\mathbb{Q}$ of rational numbers in the above. The ring $\mathbb{Q}[\sqrt{d}]$ is a field when d is not a perfect square, but whether or not it is a field it has an identity automorphism as well as an automorphism of order 2 that maps $u+v\sqrt{d}$ to $u-v\sqrt{d}$. If we restrict to integral u and v, and reduce modulo p, then one of these two automorphisms will give rise to the Frobenius map of $\mathbb{F}_p[\sqrt{d}]$.

1.2 The Artin Symbol in Abelian Extensions

We next consider the situation for higher degree extensions. Instead of x^2-d we consider any non–zero polynomial $f(x) \in \mathbb{Z}[x]$ of positive degree n and with leading coefficient 1. Instead of $d \neq 0$ we require that f have no repeated factors or, equivalently, that its discriminant $\Delta(f)$ be nonzero. Instead of $\mathbb{F}_p[\sqrt{d}]$ for a prime number p, we consider the ring $\mathbb{F}_p[\alpha]$ consisting of all p^n formal expressions

$$u_0 + u_1\alpha + u_2\alpha^2 + \ldots + u_{n-1}\alpha^{n-1}$$

with coefficients $u_i \in \mathbb{F}_p$, the ring operations being the natural ones with $f(\alpha) = 0$. Here the coefficients of $f(x)$, which are integers, are interpreted in $\mathbb{F}_p$, as before. Formally, one may define $\mathbb{F}_p[\alpha]$ to be the quotient ring $\mathbb{F}_p[x]/f(x)\mathbb{F}_p[x]$. In the same manner, replacing $\mathbb{F}_p$ by $\mathbb{Q}$ we define the ring $\mathbb{Q}[\alpha]$. It is a field if and only if $f(x)$ is irreducible.

We now need to make an important assumption, which is automatic for $n \leq 2$, but not for $n \geq 3$. Namely, instead of two automorphisms, we assume that a finite abelian group G of ring automorphisms of $\mathbb{Q}[\alpha]$ is given such that we have an equality

$$f(x) = \prod_{\sigma \in G} (x - \sigma(\alpha))$$

of polynomials with coefficients in $\mathbb{Q}[\alpha]$. This is a serious restriction. For example, in the important case that $f(x)$ is irreducible it is equivalent to $\mathbb{Q}[\alpha]$ being a Galois extension of $\mathbb{Q}$ with an abelian Galois group. Just as in the quadratic case, the Frobenius map of $\mathbb{F}_p[\alpha]$ is for almost all p induced by a unique element of the group G. The precise statement is as follows.

Theorem 1.2.1. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial such that* $\mathrm{Gal}(f) = \mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})$ *is abelian, and p be a prime number not dividing $\Delta(f)$. Then there is a unique element $\varphi_p \in \mathrm{Gal}(f)$ such that the Frobenius map of the ring $\mathbb{F}_p[\alpha]$ is the reduction of φ_p modulo p; this means that, in the ring $\mathbb{Q}[\alpha]$, one has*

$$\alpha^p = \varphi_p(\alpha) + p \cdot (q_0 + q_1\alpha + \cdots + q_{n-1}\alpha^{n-1})$$

for certain rational numbers $q_0, \ldots, q_{n-1}$ of which the denominators are not divisible by p.

Proof. Follows from the definition of the Frobenius element given in Section 1.6 and from Proposition 1.6.2. □

In all our examples, the condition on the denominators of the q_i is satisfied simply because the q_i are integers, in which case α^p and $\varphi_p(\alpha)$ are visibly *congruent* modulo p. However, there are cases in which the coefficients of $\varphi_p(\alpha)$ have a true denominator, so that the q_i will have denominators as well. Requiring the latter to be not divisible by p prevents us from picking any $\varphi_p \in G$ and just defining the q_i by the equation in the theorem.

The element φ_p of G is referred to as the *Artin symbol* of p. In the case $n = 2$ it is virtually identical to the Legendre symbol $\left(\frac{\Delta(f)}{p}\right)$. Note that for

$f(x) = x^2 - d$ we have $\Delta(f) = 4d$ so the condition that p does not divide $\Delta(f)$ is in this case equivalent to p not dividing $2d$. We can now say that, for the ring $\mathbb{F}_p[\alpha]$ occurring in Theorem 1.2.1, knowing the Frobenius map is equivalent to knowing the Artin symbol φ_p in the group G. The *Artin Reciprocity Law* imposes strong restrictions on how φ_p varies over G as p ranges over all prime numbers not dividing $\Delta(f)$ and in this way it helps us in determining the Frobenius map. Let us consider an example to illustrate it.

Example 1.2.2. *Let $f(x) = 8x^3+4x^2-4x-1$. It is an irreducible polynomial with discriminant $\Delta(f) = 2^6{\cdot}7^2$. Since the discriminant is a square,* $\mathrm{Gal}(f) \simeq C_3$ *is abelian. Our ring $\mathbb{Q}[\alpha]$ turns out to have an automorphism σ with*

$$\sigma(\alpha) = 2\alpha^2 - 1,$$

and an automorphism $\tau = \sigma^2$ with

$$\tau(\alpha) = \sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(2\alpha^2 - 1) = (1 - 2\alpha - 4\alpha^2) \cdot 2^{-1};$$

here we used the defining relation $8\alpha^3 + 4\alpha^2 - 4\alpha - 1 = 0$ that is $\alpha^3 = (-4\alpha^2 + 4\alpha + 1) \cdot 8^{-1}$. One checks that σ and τ constitute, together with the identity automorphism, a group of order 3 that satisfies the condition $f(x) = (x - \alpha)(x - \sigma(\alpha))(x - \tau(\alpha))$. Let us compute some of the Artin symbols φ_p for primes $p \neq 2, 7$. We have

$$\alpha^3 = (1 + 4\alpha - 4\alpha^2) \cdot 8^{-1} \equiv (1 - 2\alpha - 4\alpha^2) \cdot 2^{-1} = \tau(\alpha) \pmod 3,$$

so $\varphi_3 = \tau$. Likewise,

$$\alpha^5 = \frac{3}{32} + \frac{5}{16}\alpha - \frac{1}{2}\alpha^2 \equiv 2\alpha^2 - 1 = \sigma(\alpha) \pmod 5,$$

so $\varphi_5 = \sigma$. A small computation yields

$$\alpha^{11} = \frac{89}{2048} + \frac{131}{1024}\alpha - \frac{155}{512}\alpha^2 \equiv (1 - 2\alpha - 4\alpha^2) \cdot 2^{-1} = \tau(\alpha) \pmod{11},$$

so $\varphi_{11} = \tau$. Continuing in this way, one can list the value of φ_p for a few small p. The existence of such element follows from Theorem 1.2.1.

Table 1.1 can easily be computed, writing a simple loop in Maple code. As we will see later, we could instead apply Artin's reciprocity law.

Remark 1.2.3. *There is an easy pattern in Table 1.1; looking at odd primes* $p \pmod{14}$ *we have the following scenary:*

1. $p \equiv \pm 1 \pmod{14} \Rightarrow \varphi_p = 1$*;*
2. $p \equiv \pm 3 \pmod{14} \Rightarrow \varphi_p = \tau$*;*
3. $p \equiv \pm 5 \pmod{14} \Rightarrow \varphi_p = \sigma$*;*

We will explain this striking behaviour in the next section.

p	3	5	11	13	17	19	23	29	31	37	41	43
φ_p	τ	σ	τ	1	τ	σ	σ	1	τ	σ	1	1
p	47	53	59	61	67	71	73	79	83	89	97	101
φ_p	σ	τ	τ	σ	τ	1	τ	σ	1	σ	1	τ

Table 1.1: Artin symbol for odd primes p such that $p \leq 101$, with $p \neq, 7$.

Artin symbols are worth knowing because they control much of the arithmetic of $\mathbb{Q}[\alpha]$. They tell us in which way the polynomial $f(x)$ with $f(\alpha) = 0$ factors modulo the prime numbers coprime to $\Delta(f)$. This gives strong information about the prime ideals of the ring $\mathbb{Z}[\alpha]$, which for $\mathbb{Z}[\alpha]$ are just as important as the prime numbers themselves are for $\mathbb{Z}$. Here are two illustrative results.

Theorem 1.2.4. *Let* $f(x) \in \mathbb{Z}[x]$ *be an irreducible polynomial,* $G = \mathrm{Gal}(f)$ *be abelian, and* p *be a prime number not dividing* $\Delta(f)$*. Then the degree of any irreducible factor of* $(f \bmod p)$ *in* $\mathbb{F}_p[x]$ *is equal to the order of* φ_p *in the group* G*. In particular, one has* $\varphi_p = id$ *in* G *if and only if* $(f \bmod p)$ *splits into* n *linear factors in* $\mathbb{F}_p[x]$*.*

A direct consequence of Theorem 1.2.4 is, for $n \geq 3$, that all irreducible factors of $(f \bmod p)$ have the same degree. This illustrates the strength of our assumptions. In the case $f(x) = x^2 - d$, Theorem 1.2.4 implies that one has $\left(\frac{d}{p}\right) = +1$ if and only if d is congruent to a square modulo p. We give a proof of the theorem above in the special case of cyclotomic polynomials. The following result is taken from [LN94].

Theorem 1.2.5. *Let Φ_n be the n–th cyclotomic polynomial and p be a prime number coprime to n. Then $(\Phi_n \bmod p)$ splits in $\varphi(n)/d$ distinct monic irreducible polynomials in $\mathbb{F}_p[x]$ of the same degree d, where d is the minimum positive integer such that $p^d \equiv 1 \pmod{n}$.*

Proof. Let η be the n–th root of unity on $\mathbb{F}_p$; then $\eta \in \mathbb{F}_{p^k} \Leftrightarrow \eta^{p^k} - \eta = 0$, that is $\eta^{p^k} = \eta$, and so $p^k \equiv 1 \pmod{n}$. Now, let d be as in the statment; $p^d \equiv 1 \pmod{n} \Rightarrow \eta \in \mathbb{F}_{p^d}$, and $\nexists \mathbb{F} \subset \mathbb{F}_{p^d}$ such that $\eta \in \mathbb{F}$. Hence the minimum polynomial of η on $\mathbb{F}_p$ has degree d and, since η is an arbitrary n–th root of unity, we have the statment. □

Remark 1.2.6. *In Section 1.4 we will see that, for a cyclotomic extension, the Artin symbol is a tautology; φ_p maps ζ_n into ζ_n^p, and therefore $\mathrm{ord}(\varphi_p)$ is just the minimum positive integer d such that $p^d \equiv 1 \pmod{n}$.*

Corollary 1.2.7. *Let p be a prime number such that $p \equiv 1 \pmod{n}$. Then Φ_n splits into $\partial\Phi_n = \varphi(n)$ linear factor on $\mathbb{F}_p[x]$.*

Example 1.2.8. *Let $f(x) = x^4 + x^3 + x^2 + x + 1$ be the 5–th cyclotomic polynomial. Then we can determine the decomposition type of $(f \bmod p)$ by means of φ_p. If we identify $\mathrm{Gal}(f) = \{\sigma_j : a \mapsto a^j,$ for $1 \leq j \leq 4\}$ with $(\mathbb{Z}/5\mathbb{Z})^*$, we have a very explicit description of the fact.*

1. $p \equiv 1 \bmod 5 \Rightarrow \varphi_p = \sigma_1 \Rightarrow (f \bmod p) = (1)(1)(1)(1)$;
2. $p \equiv 2 \bmod 5 \Rightarrow \varphi_p = \sigma_2 \Rightarrow (f \bmod p) = (4)$;
3. $p \equiv 3 \bmod 5 \Rightarrow \varphi_p = \sigma_3 \Rightarrow (f \bmod p) = (4)$;
4. $p \equiv 4 \bmod 5 \Rightarrow \varphi_p = \sigma_4 \Rightarrow (f \bmod p) = (2)(2)$;

In general, the set of prime p such that $f(x)$ splits modulo p can be described by congruences conditions with respect to a modulus depending only on $f(x)$ if and only if $\mathrm{Gal}(f)$ is an abelian group. In fact, the non–abelian case is more difficult to describe. For more details on this fact, see [Wym72].

1.3 Quadratic Reciprocity

To illustrate Artin's reciprocity law, it is useful to go back to the quadratic ring $\mathbb{Q}(\sqrt{d})$. In that case knowing φ_p is equivalent to knowing $\left(\frac{d}{p}\right)$, and Artin's reciprocity law is just a disguised version of the *quadratic reciprocity law.* The latter states that for any two distinct odd prime numbers p and q one has:

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \pmod 4 \\ \left(\frac{-p}{q}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

The law is a theorem; it is the *theorema fundamentale* from Gauss's *Disquisitiones arithmeticae* (1801). Gauss also proved the *supplementary laws*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

and

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

The first one is immediate from the definition

$$\left(\frac{d}{p}\right) \equiv d^{(p-1)/2} \pmod p$$

given in Section 1.1, also called *Euler's Criterion.*

For our purposes it is more convenient to use a different formulation of the quadratic reciprocity law. It goes back to Euler, who empirically discovered the law in the 1740's but was unable to prove it.

Theorem 1.3.1 (Euler's quadratic reciprocity law). *Let d be an integer, and let p and q be prime numbers not dividing $2d$. Then we have*

$$\begin{array}{llll} p \equiv & q & \pmod{4d} & \Rightarrow \left(\frac{d}{p}\right) = \left(\frac{d}{q}\right) \\ p \equiv & -q & \pmod{4d} & \Rightarrow \left(\frac{d}{p}\right) = \operatorname{sgn}(d) \cdot \left(\frac{d}{q}\right) \end{array}$$

Euler's quadratic reciprocity law carries substantially the same information as the results of Gauss that we stated. The cases $d = -1$ and $d = 2$ are immediately clear from the supplementary laws. Then, one can use Euler's formulation to deduce Gauss's version, by simply choosing $d = (q \pm p)/4$, the sign being such that d is an integer. For example, if $p \equiv q \pmod{4d}$ and $p \equiv 1 \pmod 4$, then $p - q = 4d$ and

$$\begin{aligned} \left(\frac{q}{p}\right) &= \left(\frac{p-4d}{p}\right) \\ &= \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) \\ &= \left(\frac{-1}{p}\right)\left(\frac{d}{q}\right) \\ &= \left(\frac{-1}{p}\right)\left(\frac{q+4d}{q}\right) \\ &= \left(\frac{p}{q}\right), \end{aligned} \tag{1.2}$$

which is the first case of the quadratic reciprocity law. By means of analogous tricks, if $p \equiv 3 \pmod 4$, then one gets

$$\begin{aligned} \left(\frac{q}{p}\right) &= \left(\frac{p-4d}{p}\right) \\ &= \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) \\ &= \left(\frac{-1}{p}\right)\left(\frac{d}{q}\right) \\ &= \left(\frac{-1}{p}\right)\left(\frac{q+4d}{q}\right) \\ &= \left(\frac{-1}{p}\right)\left(\frac{p}{q}\right), \\ &= \left(\frac{-p}{q}\right). \end{aligned} \tag{1.3}$$

Not only did Euler observe that the value of the quadratic symbol $\left(\frac{d}{p}\right)$ depends only on (p mod $4d$), he also noticed that $\left(\frac{d}{p}\right)$ exhibits multiplicative properties as a function of p. For example, if p, q, j are primes satisfying $p \equiv qj \pmod{4d}$, then we have $\left(\frac{d}{p}\right) = \left(\frac{d}{q}\right) \cdot \left(\frac{d}{j}\right)$. Formulated in modern language, this leads to a special case of Artin reciprocity. Denote, for a non–zero integer m, by $(\mathbb{Z}/m\mathbb{Z})^*$ the multiplicative group of invertible elements of the ring $\mathbb{Z}/m\mathbb{Z}$. Let d again be any non–zero integer.

Theorem 1.3.2 (Artin quadratic reciprocity law). *There exists a group homomorphism*

$$\begin{array}{rcl} (\mathbb{Z}/4d\mathbb{Z})^* & \to & \{\pm 1\} \\ (p \bmod 4d) & \mapsto & \left(\dfrac{d}{p}\right) \end{array} \tag{1.4}$$

for any prime p not dividing $4d$.

If we wish to generalize Artin's quadratic reciprocity law to higher degree abelian polynomial it is natural to guess that $4d$ is to be replaced by $\Delta(f)$, and $\left(\frac{d}{p}\right)$ by φ_p. This guess is correct. Let the polynomial $f(x)$, the ring $\mathbb{Q}[\alpha]$, the abelian group $G = \mathrm{Gal}(f)$, and the Artin symbols φ_p for p not dividing $\Delta(f)$ be as in Theorem 1.2.1.

Theorem 1.3.3 (Artin reciprocity law over $\mathbb{Q}$). *There exists a group homomorphism*

$$\begin{array}{rcl} (\mathbb{Z}/\Delta(f)\mathbb{Z})^* & \to & \mathrm{Gal}(f) \\ (p \bmod \Delta(f)) & \mapsto & \varphi_p \end{array}$$

for any prime number p not dividing $\Delta(f)$.

From Theorem 1.2.4 we know that φ_p determines the splitting behavior of the polynomial $f(x)$ modulo p, so Artin reciprocity yields a relation between (f mod p) and (p mod $\Delta(f)$).

In our cubic example $f(x) = 8x^3 + 4x^2 - 4x - 1$ we have $\Delta(f) = 2^6 \cdot 7^2$ and

G is of order 3. Thus, the reciprocity law implies that the Table 1.1 of Artin symbols that we gave for $f(x)$ is periodic with period dividing $\Delta(f)$, namely with period 14 as we observed in Remark 1.2.3. It is a general phenomenon for higher degree abelian extensions that the number $\Delta(f)$ in Theorem 1.3.3 can be replaced by a fairly small divisor.

Theorems 1.3.2 and 1.3.3 are simple reformulations of the Artin reciprocity law. The original statement involves the notion of *ray class group*, which we do not discuss in this work.

We state the law as formulated in [Wym72].

Theorem 1.3.4 (Artin Reciprocity Law). *Let $L/\mathbb{Q}$ be a finite abelian extension with Galois group G, and let Γ be the subgroup of $\mathbb{Q}^*$ generated by the primes unramified in L. Then the Artin symbol gives a surjective group homomorphism*

$$\varphi : \Gamma \mapsto Gal(L/\mathbb{Q})$$

whose kernel contains the ray group Γ_a, where a is an appropriate product of the ramified primes.

In theorems 1.3.2 and 1.3.3 we replace Γ with $(\mathbb{Z}/\Delta(f)\mathbb{Z})^*$ so that we express primes in terms of congruences modulo $\Delta(f)$, and, in this way, we automatically exclude ramified primes. Moreover, this presentation gives an explicit description of the Artin symbol φ_p just looking at (p mod $\Delta(f)$).

1.4 Cyclotomic Extensions

Artin's reciprocity law over $\mathbb{Q}$ generalizes the quadratic reciprocity law. This generality depends on the study of *cyclotomic extensions.*

Let m be a positive integer, and define inductively the m–th cyclotomic polynomial $\Phi_m(x) \in \mathbb{Z}[x]$ to be the product

$$\Phi_m(x) = \frac{x^m - 1}{\prod_{d|m, d\neq m} \Phi_d(x)}.$$

So one readly proves the identity

$$\prod_{d|m} \Phi_d(x) = x^m - 1,$$

from which we can derive that the degree of Φ_m equals $\varphi(m) = \#(\mathbb{Z}/m\mathbb{Z})^*$. Therefore the discriminant $\Delta(\Phi_m)$ divides the discriminant of $\Delta(x^m - 1)$, which equals $\pm m^m$. For example, the discriminant of $\Phi_8(x) = x^4 + 1$, which equals 2^8, divides $\Delta(x^8 - 1) = -2^{24}$. Denoting by ζ_m a formal zero of $\Phi_m(x)$ we obtain a ring $\mathbb{Q}[\zeta_m]$ that has vector space dimension $\varphi(m)$ over $\mathbb{Q}$. We have $\zeta_m^m = 1$, but $\zeta_m^d \neq 1$ when $d < m$ divides m, so the multiplicative order of ζ_m equals m. In the polynomial ring over $\mathbb{Q}[\zeta_m]$ the identity

$$\Phi_m(x) = \prod_{a \in (\mathbb{Z}/m\mathbb{Z})^*} (x - \zeta_m^a)$$

is valid. One deduces that for each $a \in (\mathbb{Z}/m\mathbb{Z})^*$ the ring $\mathbb{Q}[\zeta_m]$ has an automorphism $\phi_a : \zeta_m \mapsto \zeta_m^a$ and that $G = \{\phi_a \text{ s.t. } a \in (\mathbb{Z}/m\mathbb{Z})^*\}$ is a group isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$; in particular, it is abelian. This places us in the situation of Theorem 1.2.1 with $f = \Phi_m$ and $\alpha = \zeta_m$. Applying the theorem, we find $\varphi_p = \phi_p$ for all primes p not dividing m: all q_i in the theorem vanish, Artin's reciprocity law is now almost a tautology. If we identify G with $(\mathbb{Z}/m\mathbb{Z})^*$, the Artin map

$$(\mathbb{Z}/\Delta(\Phi_m)\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z})^*$$

is simply the map

$$(a \bmod \Delta(\Phi_m)) \mapsto (a \bmod m)$$

whenever a is coprime to m. This map is clearly surjective.

We conclude that for cyclotomic extensions, Artin's reciprocity law can be proved by means of a plain verification. One can now attempt to prove Artin's reciprocity law in other cases by reduction to the cyclotomic case. For example, the supplementary law that gives the value of $\left(\frac{2}{p}\right)$ is a consequence of the fact that $\zeta_8 + \zeta_8^{-1}$ is a square root of 2. Namely, one has

$$\varphi_p(\sqrt{2}) = \varphi_p(\zeta_8 + \zeta_8^{-1}) \equiv (\zeta_8 + \zeta_8^{-1})^p \equiv \zeta_8^p + \zeta_8^{-p} \pmod{p};$$

for $p \equiv \pm 1 \pmod 8$, this equals

$$\zeta_8 + \zeta_8^{-1} = \sqrt{2},$$

and for $p \equiv \pm 3 \pmod 8$ it is

$$\zeta_8^3 + \zeta_8^{-3} = \zeta_8^4 \cdot (\zeta_8 + \zeta_8^{-1}) = -\sqrt{2}.$$

This confirms that in the two respective cases one has $\left(\frac{2}{p}\right) = 1$ and $\left(\frac{2}{p}\right) = -1$. Our example $f(x) = 8x^3 + 4x^2 - 4x - 1$ can also be reduced to the cyclotomic case: if ζ_{14} is a zero of Φ_{14} then a computation shows that

$$\alpha = (\zeta_{14}^2 + \zeta_{14}^{-2})/2 = (\zeta_{14}^2 - \zeta_{14}^5)/2$$

is a zero of f, and one finds

$$\varphi_p(\alpha) = (\zeta_{14}^{2p} + \zeta_{14}^{-2p})/2 = (\zeta_{14}^{2p} - \zeta_{14}^{5p})/2.$$

As consequence of this fact, by more simple computations we have

$$\varphi_p(\alpha) \equiv \begin{cases} (\zeta_{14}^2 - \zeta_{14}^5)/2 & = \alpha \quad \text{for } p \equiv \pm 1 \pmod{14}, \\ (-1 - \zeta_{14}^2 + \zeta_{14}^3 - \zeta_{14}^4 + \zeta_{14}^5)/2 & = \tau(\alpha) \quad \text{for } p \equiv \pm 3 \pmod{14}, \\ (\zeta_{14}^4 - \zeta_{14}^3)/2 & = \sigma(\alpha) \quad \text{for } p \equiv \pm 5 \pmod{14}. \end{cases}$$

This proves our remark on the pattern underlying the Table 1.1 of Artin symbols. The theorem of Kronecker–Weber (1887) implies that the reduction to cyclotomic extensions will always be successful: this theorem asserts that every abelian Galois extension of $\mathbb{Q}$ can be embedded in a cyclotomic extension. That takes care of the case in which $f(x)$ is irreducible, from which the general case follows easily. In particular, to prove the quadratic reciprocity law it suffices to express square roots of integers in terms of roots of unity, as we just did with $\sqrt{2}$.

1.5 Dedekind Domains

In the previous sections we gave an explicit description of the Artin symbol relative to a prime number just in terms of congruences, that is, exploiting informations based on Artin reciprocity. Here we provide an overview of the general construction of the Artin symbol, which is a fundamental tool in order to understand the Chebotarëv Theorem. We put ourselves in a more general contest, that is, the one of *Dedekind Domains*. The basic theory on Dedekind Domains, which we take for granted, can be found in [ST02].

Definition 1.5.1. *A Dedekind Domain A is a ring that satisfies the following properties:*

(a) *A is a domain, with field of fractions K;*

(b) *A is noetherian, that is, every ideal in A is finitely generated;*

(c) *A is such that if α satisfies a monic polynomial equation with coefficients in A then $\alpha \in A$;*

(d) *every non–zero prime ideal of A is maximal.*

In this section we will use the following notations: we denote by A a Dedekind domain with field of fractions K, and with B the integral closure of A in a finite separable extension L of K. It will be useful to think of the simplest example for which these relations hold, namely $A = \mathbb{Z}$, $K = \mathbb{Q}$, $B = \mathcal{O}_L$, where $\mathcal{O}_L$ is the set of elements of L whose monic minimum polynomial has coefficients in $\mathbb{Z}$; this set make up the ring of *algebraic integers* in L. The ring $\mathcal{O}_L$ is a Dedekind domain when L/K is a finite extension of the number field K. We recall the notion of division between ideals.

Definition 1.5.2. *For ideals $\mathfrak{a}$, $\mathfrak{b}$ of A, we say that*

$$\mathfrak{a}|\mathfrak{b} \Leftrightarrow \mathfrak{a} \supseteq \mathfrak{b}.$$

Let $\mathfrak{p}$ be a nonzero prime ideal of A. Then $\mathfrak{p}B$ is an ideal of B, and it has a factorization

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g},\ e_i > 0,$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ are distinct prime ideals of B, and $e_1, \ldots, e_g$ are positive integers. Hence $\mathfrak{P}$ divides $\mathfrak{p}$, written $\mathfrak{P} \mid \mathfrak{p}$, if $\mathfrak{P}$ occurs in the factorization of $\mathfrak{p}B$. Primes dividing $\mathfrak{p}$ have a specific property.

Lemma 1.5.3. *A prime ideal $\mathfrak{P}$ of B divides $\mathfrak{p}$ if and only if $\mathfrak{p} = \mathfrak{P} \cap A$.*

Proof. ($\Rightarrow$) Clearly $\mathfrak{p} \subset \mathfrak{P} \cap A$; but $\mathfrak{P} \cap A \neq A$ and $\mathfrak{p}$ is maximal, so $\mathfrak{P} \cap A = \mathfrak{p}$. ($\Leftarrow$) If $\mathfrak{p} \subset \mathfrak{P}$ then $\mathfrak{p}B \subset \mathfrak{P}$, and this implies that $\mathfrak{P}$ occurs in the factorization of $\mathfrak{p}B$. □

Definition 1.5.4. *If any of the numbers e_i is > 1, then we say that $\mathfrak{p}$ is ramified in B; the number $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ is called the ramification index. We then write $f_i = f(\mathfrak{P}_i/\mathfrak{p})$ for the vector space dimension $[B/\mathfrak{P}_i : A/\mathfrak{p}]$, called the relative degree of $\mathfrak{P}_i$.*

Example 1.5.5. *Let $L = \mathbb{Q}[\sqrt{2}]$ and $K = \mathbb{Q}$; it follows that $B = \mathbb{Z}[\sqrt{2}]$ and $A = \mathbb{Z}$. The prime ideal $(2) = 2\mathbb{Z}$ has the factorization $2B = (\sqrt{2}B)^2$. It's easy to see that $\sqrt{2}B$ is a prime ideal because*

$$\sqrt{2}B = 2\mathbb{Z} + \sqrt{2}\mathbb{Z},$$

and so $B/\sqrt{2}B$ is the field of 2 elements. It follows that the ramification index $e(\mathfrak{P}/(2))$ of $\mathfrak{P} = \sqrt{2}B$ is 2, and $f(\mathfrak{P}/(2))$ is $[\mathbb{Z}[\sqrt{2}]/\sqrt{2}\mathbb{Z}[\sqrt{2}] : \mathbb{Z}/2\mathbb{Z}] = 1$, since they are both isomorphic to a field of 2 elements. Thus the prime ideal $(2) = 2\mathbb{Z}$ ramifies in $B = \mathbb{Z}[\sqrt{2}]$.

Lemma 1.5.6. *Let L/K be a finite Galois extension and $G = \mathrm{Gal}(L/K)$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and let $\mathfrak{P}_1, \mathfrak{P}_2$ be prime ideals of $\mathcal{O}_L$ dividing $\mathfrak{p}$. Then there exists $\sigma \in G$ such that $\mathfrak{P}_1 = \sigma(\mathfrak{P}_2)$.*

Proof. Suppose that $\mathfrak{P}_1 \neq \sigma(\mathfrak{P}_2), \forall \sigma \in G$. By the Chinese Reminder Theorem, there exists an element $x \in B$ such that $x \equiv 0 \pmod{\mathfrak{P}_1}$, and $x \equiv 1 \bmod \sigma(\mathfrak{P}_2), \forall \sigma \in G$. The element

$$N(x) := \prod_{\sigma \in G} \sigma(x)$$

lies in $B \cap K = A$, and lies in $\mathfrak{P}_1 \cap A = \mathfrak{p}$, because $\mathfrak{P}_1 \mid \mathfrak{p}$. But $x \notin \sigma(\mathfrak{P}_2), \forall \sigma \in G$, so that $\sigma(x) \notin \mathfrak{P}_2, \forall \sigma \in G$. This contradicts the fact that $N(x)$ lies in $\mathfrak{p} = \mathfrak{P}_2 \cap A$. □

Theorem 1.5.7. *Let m be the degree of the field extension L/K, and let $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ be the prime ideals dividing $\mathfrak{p}$; then*

$$\sum_{i=1}^{g} e_i f_i = m.$$

Moreover, if L/K is a Galois extension, then all the ramification numbers and all the relative degrees are equal; therefore

$$efg = m.$$

Proof. See [Sam67, Chap.5]. The proof of the equality in the case of abelian extensions follows from Lemma 1.5.6. □

Definition 1.5.8. *Let L be a finite extension of degree m over $K = \mathbb{Q}$, and $\{\alpha_1, \dots, \alpha_m\}$ be a basis of L as vector space over $\mathbb{Q}$. We define the discriminant of this basis to be*

$$\Delta[\alpha_1, \dots, \alpha_n] = \{\det[\sigma_i(\alpha_j)]\}^2, \ i, \, j = 1, \dots m,$$

for all $\sigma_i : L \to \mathbb{C}$ such that σ_i is a K–homomorphism.

We will focus on basis for $\mathcal{O}_L$ over $\mathcal{O}_K = \mathbb{Z}$, called an *integral basis* for $\mathcal{O}_L$. If $\{\alpha_1, \dots, \alpha_m\}$ if an integral basis for $\mathcal{O}_L$, then we can prove that $\Delta[\alpha_1, \dots, \alpha_n]$ is a rational integer and that if $\{\beta_1, \dots, \beta_n\}$ is another integral basis for $\mathcal{O}_L$, then $\Delta[\beta_1, \dots, \beta_n] = \Delta[\alpha_1, \dots, \alpha_n]$. For the proof of these facts, see [ST02, Chap.2].

The following gives a description of the prime ideals that ramify in an extension.

Theorem 1.5.9. *A prime ideal $\mathfrak{p} = p\mathbb{Z} \in \mathcal{O}_K = \mathbb{Z}$ ramifies in $\mathcal{O}_L$ if and only if $p \mid \Delta(\mathcal{O}_L/\mathbb{Z})$. In particular, only finitely many prime ideals ramify.*

Proof. See [Sam67, Chap.5]. □

In other words, a prime ideal $p \in \mathbb{Z}$ ramifies in $\mathcal{O}_L$ if and only if p contains the ideal $(\Delta(\mathcal{O}_L/\mathbb{Z}))$.

Example 1.5.10. *Let* $L = \mathbb{Q}[\sqrt{-2}]$ *and* $\mathcal{O}_L = \mathbb{Z}[\sqrt{-2}]$ *so that* $\Delta(\mathbb{Z}[\sqrt{-2}]/\mathbb{Z})$ *equals*

$$\begin{vmatrix} 1 & \sqrt{-2} \\ 1 & -\sqrt{-2} \end{vmatrix} = -8.$$

If p *is an odd prime, then* p *does not ramify. By Theorem 1.5.7 we have* $2 = fg$*. Let* $p = 3$*; then* $g = 2$ *and* $f = 1$*. In fact,* $3\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2$*, where* $\mathfrak{P}_1 = (3, 1 + \sqrt{-2})$ *and* $\mathfrak{P}_2 = (3, 1 - \sqrt{-2})$*. Notice that* $\mathfrak{P}_2 = \sigma\mathfrak{P}_1$*, with* $\mathrm{Gal}(\mathbb{Q}(\sqrt{-2})/\mathbb{Q}) \ni \sigma = conj : \sqrt{-2} \mapsto -\sqrt{-2}$*, as Lemma 1.5.6 predicts. In these conditions, we must obtain* $f = 1$*; in fact* $f = [\frac{\mathbb{Z}[\sqrt{-2}]}{\mathfrak{P}_i} : \frac{\mathbb{Z}}{3\mathbb{Z}}] = 1$*, because* $\mathbb{Z}[\sqrt{-2}]/\mathfrak{P}_i = \{a + b\sqrt{-2} \text{ s.t. } a \equiv b \bmod 3 \text{ and } a, b \in \mathbb{Z}_3\}$*, which is isomorphic to* $\mathbb{Z}/3\mathbb{Z}$*.*

1.6 The Frobenius Element

For the theory developed in this section we refer to [Sam67, Chap.6]. We keep the same notations of last section: let A be a Dedekind Domain, K be its quotient field, and L be a finite Galois extension of K with $\mathrm{Gal}(L/K) = G$. Let $\mathfrak{p}$ be a prime ideal of A, and $\mathfrak{P}$ be an ideal of $B = \mathcal{O}_L$ dividing $\mathfrak{p}$. We denote $F_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P} = B/\mathfrak{P}$ and $F_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p} = A/\mathfrak{p}$.

Definition 1.6.1. *The decomposition group* $G(\mathfrak{P})$ *of* $\mathfrak{P}$ *is defined to be*

$$\{\sigma \in G \text{ s.t. } \sigma\mathfrak{P} = \mathfrak{P}\}.$$

Then $G(\mathfrak{P})$ acts in a natural way on the residue class field $F_{\mathfrak{P}}$, and leaves $F_{\mathfrak{p}}$ fixed. To each $\sigma \in G(\mathfrak{P})$ we can associate an automorphism $\bar{\sigma}$ of $F_{\mathfrak{P}}$ over $F_{\mathfrak{p}}$, and the map given by

$$\sigma \longmapsto \bar{\sigma}$$

induces a homomorphism of $G(\mathfrak{P})$ into the group of automorphism of $F_{\mathfrak{P}}$.

Proposition 1.6.2. *Let* L/K *be a finite Galois extension, with* $G = \mathrm{Gal}(L/K)$*. Let* $\mathfrak{p}$ *be a prime ideal and* $\mathfrak{P}$ *such that* $\mathfrak{P} \mid \mathfrak{p}$*. Then* $F_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$ *is a Galois* *extension of* $F_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ *and the map* $\sigma \mapsto \bar{\sigma}$ *induces a surjective homomorphism of* $G(\mathfrak{P})$ *into the Galois group* $\mathrm{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}})$*.*

Proof. Let $A = \mathcal{O}_K$ and $B = \mathcal{O}_L$. Let $L^{G(\mathfrak{P})}$ be the field of invariants of L under the action of the decomposition group of $\mathfrak{P}$, $\bar{A}^{L^{G(\mathfrak{P})}} = B \cap L^{G(\mathfrak{P})}$ be the integral closure of A in $L^{G(\mathfrak{P})}$, $\mathfrak{P}_{G(\mathfrak{P})} = \mathfrak{P} \cap \bar{A}^{L^{G(\mathfrak{P})}}$. $\mathfrak{P}$ is the only prime factor of $B\mathfrak{P}_{G(\mathfrak{P})}$. In fact, if $\mathfrak{P}_1$ is another prime ideal dividing $B\mathfrak{P}_{G(\mathfrak{P})}$, then $\mathfrak{P}_{G(\mathfrak{P})} = \mathfrak{P}_1 \cap \bar{A}^{L^{G(\mathfrak{P})}}$ by Lemma 1.5.3, while $\mathfrak{P}_{G(\mathfrak{P})} = \mathfrak{P} \cap \bar{A}^{L^{G(\mathfrak{P})}}$. But, by Theorem 1.5.6, there exists an element $\sigma \in \mathrm{Gal}(L/L^{G(\mathfrak{P})}) = G(\mathfrak{P})$ such that $\sigma\mathfrak{P} = \mathfrak{P}_1$; since any σ in $G(\mathfrak{P})$ fixes $\mathfrak{P}$, the equality $\mathfrak{P}_1 = \mathfrak{P}$ holds. We set $B\mathfrak{P}_{G(\mathfrak{P})} = \mathfrak{P}^{e'}$ and denote with f' the relative degree $[B/\mathfrak{P} : \bar{A}^{L^{G(\mathfrak{P})}}/\mathfrak{P}_{G(\mathfrak{P})}]$. Hence $\mathrm{Gal}(L/L^{G(\mathfrak{P})}) = G(\mathfrak{P})$ and

$$e'f' = [L : L^{G(\mathfrak{P})}] = \#G(\mathfrak{P}) = ef.$$

Since $A/\mathfrak{p} \subset \bar{A}^{L^{G(\mathfrak{P})}}/\mathfrak{P}_{G(\mathfrak{P})} \subset B/\mathfrak{P}$, we have $f' \leq f$, and $e' \leq e$ because of $p\bar{A}^{L^{G(\mathfrak{P})}} \subset \mathfrak{P}_{G(\mathfrak{P})}$; but $e'f' = ef$, so that $e = e'$ and $f = f'$. Therefore

$$A/\mathfrak{p} \simeq \bar{A}^{L^{G(\mathfrak{P})}}/\mathfrak{P}_{G(\mathfrak{P})}.$$

Let $\bar{\alpha}$ be a primitive element of $B/\mathfrak{P}$ on $A/\mathfrak{p}$ and $\alpha \in B$ be a representing element of $\bar{\alpha}$. If $x^r + a_{r-1}x^{r-1} + \cdots + a_0$ is the minimal polynomial of α on $L^{G(\mathfrak{P})}$, then $a_i \in \bar{A}^{L^{G(\mathfrak{P})}}$ and the set of its root is $\{\sigma(\alpha) \text{ s.t. } \sigma \in G(\mathfrak{P})\}$. From the isomorphism $A/\mathfrak{p} \simeq \bar{A}^{L^{G(\mathfrak{P})}}/\mathfrak{P}_{G(\mathfrak{P})}$, we can consider the reduced polynomial in $A/\mathfrak{p}$, whose set of roots is $\{\bar{\sigma}(\bar{\alpha}) \text{ s.t. } \sigma \in G(\mathfrak{P})\}$. On the one hand we conclude that $B/\mathfrak{P}$ contains all the conjugates of $\bar{\alpha}$ in $A/\mathfrak{p}$, hence $B/\mathfrak{P}$ is a Galois extension of $A/\mathfrak{p}$. On the other hand, since any conjugate of $\bar{\alpha}$ in $A/\mathfrak{p}$ is of the form $\bar{\sigma}(\bar{\alpha})$, any $A/\mathfrak{p}$–automorphism of $B/\mathfrak{P}$ is a $\bar{\sigma}$. Finally, the Galois group of $B/\mathfrak{P}$ on $A/\mathfrak{p}$ is identified with $G(\mathfrak{P})/T(\mathfrak{P})$ and, since $[B/\mathfrak{P} : A/\mathfrak{p}] = f$, we have $\#G(\mathfrak{P})/\#T(\mathfrak{P}) = f$, that is $\#T(\mathfrak{P}) = e$. □

Definition 1.6.3. *The Inertia group* $T(\mathfrak{P})$ *of* $\mathfrak{P}$ *is defined to be the kernel of the homomorhism* $\sigma \mapsto \bar{\sigma}$*.*

We recall that in the case L/K abelian of degree n, it holds $n = efg$, and $\#G(\mathfrak{P}) = n/g = ef$; moreover, from Proposition 1.6.2,

$$\frac{G(\mathfrak{P})}{T(\mathfrak{P})} \simeq \mathrm{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}}),$$

and so $f = \#G(\mathfrak{P})/\#T(\mathfrak{P})$, that is $\#T(\mathfrak{P}) = e$.

Corollary 1.6.4. *The prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ is not ramified in $\mathcal{O}_L$ if and only if $T(\mathfrak{P})$ is trivial, for any prime ideal $\mathfrak{P}$ dividing $\mathfrak{p}$.*

Thus, assume that $\mathfrak{p}$ is unramified and that $\mathfrak{P} \mid \mathfrak{p}$. Then $\mathrm{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}})$ is cyclic with a canonical generator, namely, the Frobenius automorphism $x \longrightarrow x^q$, where q is the number of elements of $F_{\mathfrak{p}}$. Hence $T(\mathfrak{P})$ is trivial and $G(\mathfrak{P})$ is cyclic. The generator of $G(\mathfrak{P})$ corresponding to the Frobenius automorphism in $\mathrm{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}})$ deserves a special name.

Definition 1.6.5. *We define the Frobenius element $\sigma_{\mathfrak{P}} = (\mathfrak{P}, L/K)$ of $\mathfrak{P}$ to be the element of $G(\mathfrak{P})$ that acts as the Frobenius automorphism on the residue field extension $F_{\mathfrak{P}}/F_{\mathfrak{p}}$.*

Therefore the Frobenius element $\sigma \in \mathrm{Gal}(L/K)$ is uniquely determined by the following two conditions:

1. $\sigma \in G(\mathfrak{P}),$ that is $\sigma\mathfrak{P} = \mathfrak{P}$;

2. for all $\alpha \in \mathcal{O}_L,\ \sigma(\alpha) \equiv \alpha^q \pmod{\mathfrak{P}}$, where q is the number of elements of the residue field $F_{\mathfrak{p}}$, with $\mathfrak{p} = \mathfrak{P} \cap K$.

We now list the basic properties of $(\mathfrak{P}, L/K)$.

Proposition 1.6.6. *Let $\sigma\mathfrak{P}$ be a second prime ideal dividing $\mathfrak{p}$, for any $\sigma \in G$. Then:*

(a) *$G(\sigma\mathfrak{P}) = \sigma G(\mathfrak{P})\sigma^{-1}$,*

(b) *$T(\sigma\mathfrak{P}) = \sigma T(\mathfrak{P})\sigma^{-1}$.*

Proof. (a) ($\subseteq$) Let $\tau \in G(\mathfrak{P})$; we have $\sigma\tau\sigma^{-1} \cdot \sigma(p) = \sigma\tau(p) = \sigma(p)$, and $\sigma G(\mathfrak{P})\sigma^{-1} \subseteq G(\sigma(\mathfrak{P}))$. ($\supseteq$) Let $\theta \in G(\sigma(\mathfrak{P}))$; $\theta{\cdot}\sigma(\mathfrak{p}) = \sigma(\mathfrak{p}) \Rightarrow \sigma^{-1}\theta{\cdot}\sigma(\mathfrak{P}) = \mathfrak{P}$, and $\sigma^{-1}\theta\sigma \in G(\mathfrak{P})$, i.e., $\theta \in \sigma^{-1}G(\mathfrak{P})\sigma$ or, equivalently, $G(\sigma(\mathfrak{P})) \subseteq \sigma^{-1}G(\mathfrak{P})\sigma$.

□

Corollary 1.6.7. *For all $\sigma \in G$ we have $(\sigma\mathfrak{P}, L/K) = \sigma(\mathfrak{P}, L/K)\sigma^{-1}$*

Proof. The equality follows from Proposition 1.6.6 and from Definition 1.6.5.

□

It's easily seen that, if $\mathrm{Gal}(L/K)$ is abelian, then $(\mathfrak{P}, L/K) = (\mathfrak{P}', L/K)$ for all primes $\mathfrak{P}, \mathfrak{P}'$ dividing $\mathfrak{p}$, and we write $\sigma_{\mathfrak{p}} = (\mathfrak{p}, L/K)$ for this element, which equals the Artin symbol discussed in the previous sections. If $\mathrm{Gal}(L/K)$ is not abelian, then $\{(\mathfrak{P}, L/K) \text{ s.t. } \mathfrak{P} \mid \mathfrak{p}\}$ is a conjugacy class in G, which, by an abuse of notation, we again denote $(\mathfrak{p}, L/K)$. So, for a prime ideal $\mathfrak{p}$ of O_K, $(\mathfrak{p}, L/K)$ is either an element of $\mathrm{Gal}(L/K)$ or a conjugacy class depending on whether $\mathrm{Gal}(L/K)$ is abelian or nonabelian.

Example 1.6.8. *Let $L = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n–th root of* 1*. If $p \mid n$ then $\mathfrak{p} = p\mathbb{Z}$ ramifies in $\mathcal{O}_L$ by Theorem 1.5.9, and $(\mathfrak{p}, L/\mathbb{Q})$ is not defined. Otherwise $\sigma = (\mathfrak{p}, L/\mathbb{Q})$ is the unique element of* $\mathrm{Gal}(L/\mathbb{Q})$ *such that*

$$\sigma(\alpha) \equiv \alpha^p \bmod \mathfrak{P},\ \forall \alpha \in \mathcal{O}_L = \mathbb{Z}[\zeta_n],$$

where $\mathfrak{P}$ ranges over the prime ideals dividing $\mathfrak{p}$. We claim that σ is the element of $\mathrm{Gal}(L/\mathbb{Q})$ *such that $\sigma(\zeta_n) = \zeta_n^p$; let $\mathfrak{P}$ be a prime ideal dividing $\mathfrak{p}$ in $\mathbb{Z}[\zeta_n]$; then modulo $\mathfrak{P}$, we have*

$$\sigma\left(\sum a_i\zeta_n^i\right) = \sum a_i\zeta_n^{ip} = \sum a_i^p\zeta_n^{ip} = \left(\sum a_i\zeta_n^i\right)^p$$

as required. Note that $(\mathfrak{p}, L/\mathbb{Q})$ has order f, where $f = f(\mathfrak{P}/\mathfrak{p})$ is the residual degree $[F_{\mathfrak{P}} : F_{\mathfrak{p}}]$.

Knowledge of the Frobenius element also allows us to control the decomposition of $\mathfrak{p}$ in $\mathcal{O}_L$. We can see it in the simple case $L = \mathbb{Q}(\gamma)$ and

$K = \mathbb{Q}$. With this assumption, $\mathfrak{p} = p\mathbb{Z}$ and $\mathrm{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}}) = \langle \varphi : a \mapsto a^p \rangle$. If α_i is a root of an irreducible factor $\bar{f}_i$ of $(f \bmod p)$, then, by Lemma A.0.7, the length of the orbit of α_i under the action of $\langle \varphi : a \mapsto a^p \rangle$ equals ∂f_i, and therefore the cycle pattern of φ contains a ∂f_i–cycle. Repeating this procedure on each irreducible factor, we get that the decomposition type of $(f \bmod p)$ equals the cycle structure of φ. Finally, in the unramified case, Theorem 1.6.2 holds and $\mathrm{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}}) \simeq G(\mathfrak{P}) \subset \mathrm{Gal}(L/K)$; so we can assume that $\mathrm{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}}) \subset \mathrm{Gal}(L/K)$ and there will be an element corrisponding to φ in $\mathrm{Gal}(L/K)$ with the same cycle structure. If we are interested in factoring pO_L, it's sufficient to compute the decomposition type of $(f \bmod p)$, by virtue of the following.

Theorem 1.6.9. *Let L be a number field of degree n with ring of integers $\mathcal{O}_L = \mathbb{Z}[\theta]$ generated by $\theta \in \mathcal{O}_K$. Given a rational prime p, suppose the minimum polynomial $f(x)$ of θ over $\mathbb{Q}$ gives rise to the factorization into irreducibles over $\mathbb{Z}_p$:*

$$\bar{f} = \bar{f_1}^{e_1} \cdots \bar{f_r}^{e_r}$$

where the bar denotes the natural map $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$. Then, if $f_i \in \mathbb{Z}[x]$ is a polynomial mapping onto $\bar{f}_i$, the ideal

$$\mathfrak{p}_i = \langle p, \, f_i(\theta) \rangle$$

is prime and the prime factorization of $\mathfrak{p}$ is

$$\mathfrak{p} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Proof. See [ST02, Chap.10]. □

For example, if $L = \mathbb{Q}(\sqrt{2})$, then $\mathcal{O}_L = \mathbb{Z}[\sqrt{2}]$ and therefore $2\mathcal{O}_L = \langle \sqrt{2} \rangle^2$.

Remark 1.6.10. *Theorem 1.6.9 holds when the ring of integers $\mathcal{O}_L$ is generated by a single element, i.e., there exists a $\theta \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathbb{Z}[\theta]$. This is not usually the case. For example, in $\mathbb{Q}(\sqrt[3]{175})$, one can show that the ring of integers is $\mathbb{Z}[\sqrt[3]{175}, \sqrt[3]{245}]$, and that it is not generated by a single element.*

To conclude this chapter we give a complete treatment of the theory developed in the case of quadratic extension.

Example 1.6.11. *Let $L = \mathbb{Q}[\sqrt{d}]$ where $d \in \mathbb{Z}$ is square–free, and let $\mathfrak{p} = p\mathbb{Z}$ be a prime ideal in $\mathbb{Z}$. Identify* $\mathrm{Gal}(L/\mathbb{Q})$ *with* $\{\pm 1\}$*. We will prove that* $(\mathfrak{p}, L/\mathbb{Q}) = +1$ *or* -1 *according as $\mathfrak{p}$ does, or does not, split in L, that is, according as d is, or is not, a square modulo p.*
In other words $(\mathfrak{p}, L/\mathbb{Q}) = \left(\frac{d}{p}\right)$*. From Theorem 1.5.7, the formula* $\sum_{i=1}^{g} e_i f_i = 2$ *shows that $g \leq 2$ and that only 3 cases occur:*

(a) $g = 2,\ e_1 = e_2 = 1,\ f_1 = f_2 = 1$*; we say that $\mathfrak{p}$ splits in L;*

(b) $g = 1,\ e_1 = 1,\ f_1 = 2$*; we say that $\mathfrak{p}$ is prime in L;*

(c) $g = 1,\ e_1 = 2,\ f_1 = 1$*; we say that $\mathfrak{p}$ is ramified in L.*

Let p be an odd prime not dividing d; there are 2 possibilities for B, that is $B = \mathbb{Z} + \sqrt{d}\mathbb{Z}$, or $B = \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z}$. Let us consider the cosets in B/pB; in the second case, $a + b\left(\frac{1+\sqrt{d}}{2}\right)$ (being b an odd number) is congruent to $a + (b+p)\left(\frac{1+\sqrt{d}}{2}\right)$, which is an element in $\mathbb{Z} + \sqrt{d}\mathbb{Z}$. Thus, whether or not b is odd, we have $B/pB \simeq (\mathbb{Z} + \sqrt{d})\mathbb{Z}/(p)$. Moreover, $\mathbb{Z} + \sqrt{d}\mathbb{Z} \simeq \mathbb{Z}[x]/(x^2 - d)$, and so

$$B/pB \simeq \mathbb{Z}[x]/(p, x^2 - d) \simeq \mathbb{Z}_p[x]/(x^2 - d).$$

Our question on the factorization of pB is actually a question on the irreducibility of $x^2 - d \in \mathbb{Z}_p[x]$, namely, on the value of the Legendre symbol $\left(\frac{d}{p}\right)$. In Section 1.1 we have seen that the Frobenius map is one of the two obvious automorphisms of $\mathbb{Z}_p[\sqrt{d}]$: for $\left(\frac{d}{p}\right) = +1$ it is the identity, and for $\left(\frac{d}{p}\right) = -1$ it is the map sending $a + b\sqrt{d}$ to $a - b\sqrt{d}$.

Chapter 2

Chebotarëv's Density Theorem

2.1 Symmetric Polynomials

The results in this chapter can be found in [Rot95] and [vdW91].

Definition 2.1.1. *A polynomial $P(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ is said to be symmetric if it is unchanged when its variables are permuted, that is, if*

$$P(x_{\sigma(1)}, \dots, x_{\sigma(n))}) = P(x_1, \dots, x_n), \ \forall \sigma \in S_n.$$

Example 2.1.2. *Let $t_1(x) = \sum x_i = x_1 + \ldots + x_n$; this is a symmetric polynomials, called the first* **elementary symmetric polynomial***. Then, let $x = (x_1, \dots, x_n)$; we define*

$$t_2(x) = \sum_{i<j} x_i x_j = x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_{n-1}x_n.$$

In general $t_r(x) = \sum_{i_1<\dots<i_r} x_{i_1} \cdots x_{i_r}$ and $t_n(x) = x_1x_2 \cdots x_n$ are the r–th and n–th elementary symmetric polynomial of x.

It's interesting to notice that if a monic polynomial $f(x) = \sum_{i=0}^n a_i x^i$ has roots $\alpha_1, \dots, \alpha_n$, then each of the coefficients a_i of $f(x) = \prod_{i=0}^n (x - \alpha_i)$ is an elementary symmetric polynomial of $\alpha = (\alpha_1, \dots, \alpha_n)$, and the following equality holds

$$f(x) = x^n - t_1(\alpha)x^{n-1} + \cdots + (-1)^n t_n(\alpha).$$

Here we give an important theorem on symmetric polynomials.

Theorem 2.1.3. *Every symmetric polynomial $P(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ is equal to a polynomial in the elementary symmetric polynomials with coefficients in $\mathbb{Z}$, i.e., $\exists Q \in \mathbb{Z}[t_1, \dots, t_n]$ s.t $P(x_1, \dots, x_n) = Q(t_1(x), \dots, t_n(x))$.*

2.2 Dedekind's Theorem

Let $\alpha_1, \dots \alpha_n$ be the roots of $f(x) \in \mathbb{Z}[x]$ and consider the expression

$$\theta = u_1\alpha_1 + \ldots + u_n\alpha_n,$$

where u_i are indeterminates. Let us consider the product

$$F(z, u) = \prod_{s \in S_n} (z - s_u(\theta)),$$

where the symbol s_u indicates that the permutation s acts on the indeterminates u_i. This product is a simmetric function of the roots, and therefore, by Section 2.1, it can be expressed in terms of the coefficients of $f(x)$. Let

$$F(z, u) = F_1(z, u)F_2(z, u) \cdots F_r(z, u)$$

be the decomposition of $F(z, u)$ into irriducibiles factors in $\mathbb{Z}[u, z]$. The permutations s_u which carry any of the factors, say F_1, into itself form a group G.

Proposition 2.2.1. *With precedent notations, $G \simeq \mathrm{Gal}(f)$.*

Proof. After adjoing all roots, F and therefore F_1 are decomposed into linear factors of the type $z - \sum u_v\alpha_v$, with the roots α_v as coefficients in any sequential order. Let F_1 such that it contains the factor $z-(u_1\alpha_1+\cdots+u_n\alpha_n)$. By s_u we shall hereafter denote any permutation of the u, and by s_α the same permutation of the α. Then the product $s_u s_\alpha$ leaves invariant the expression $\theta = u_1\alpha_1 + \ldots + u_n\alpha_n$; that is, we have

$$\begin{aligned} s_u s_\alpha \theta &= \theta \\ s_\alpha \theta &= s_u^{-1}\theta \end{aligned}$$

If s_u belongs to the group G, that is, if it leaves F_1 invariant, then s_u transforms every linear factor of F_1, including the factor $z - \theta$, into a linear factor of F_1 again. If, conversely, a permutation s_u transforms the factor $z - \theta$ into another linear factor of F_1, it transforms F_1 into a polynomial which is irreducible in $\mathbb{Z}[u, z]$ and which is a divisor of $F(z, u)$, and so it transforms F_1 into one of the polynomials F_j. This F_j has a linear factor in common with F_1. Therefore the permutation necessarily transforms F_1 into itself, which means that $s_u \in G$. Thus G consists of the permutations of the u which transform $z - \theta$ into a linear factor of F_1 again. The permutations s_α of the Galois group of $f(x)$ are characterized by the property that they transform the quantity

$$\theta = u_1\alpha_1 + \cdots + u_n\alpha_n$$

into its conjugates. This means that s_α transforms θ into an element satisfying the same irreducible equation as θ, that is, s_α carries the linear factor $z - \theta$ into another linear factor of F_1. Now, $s_\alpha\theta = s_u^{-1}\theta$; hence, s_u^{-1} carries the linear factor $z - \theta$ again into a linear factor of F_1; that is, s_u^{-1} and so s_u belong to G. The converse is also true. Thus, the Galois group consists of exactly the same permutations as the group G, excepted they are performed on the α instead of the u. □

This proposition gives an algorithm for computing the Galois group of a polynomial $f(x) \in \mathbb{Z}[x]$. First find the roots of $f(x)$ to a high degree of accuracy. Then compute $F(z, u)$ exactly, using the fact that it has coefficients in $\mathbb{Z}$. Factor $F(z, u)$, and take one of the factors $F_1(z, u)$. Finally list the elements σ of S_n such that σ fixes $F_1(z, u)$. The problem with this approach is that $F(z, u)$ has degree $n!$. Hence, from a pratical point of view, this method for determining the Galois group is not so much useful. However, the following interesting fact can be derived from it.

Lemma 2.2.2. *Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$. Let $\mathfrak{p} = p\mathbb{Z}$ be a prime ideal in $\mathbb{Z}$, and let $\bar{f}(x)$ be the image of $f(x)$ in $(\mathbb{Z}/\mathfrak{p})[x]$. Assume that neither $f(x)$ nor $\bar{f}(x)$ has a multiple root. Then the Galois group* $\mathrm{Gal}(\bar{f})$

relative to the quotient field of $\mathbb{Z}/\mathfrak{p}$ *is a subgroup of the Galois group* $\mathrm{Gal}(f)$ *relative to* $\mathbb{Q}$*.*

Proof. The factorization of

$$F(z,u) = \prod_s (z - s_u\theta)$$

into irreducibile factors in can be carried out in $\mathbb{Z}[u,z]$. The natural homomorphism carries this factorization down into $\mathbb{Z}/\mathfrak{p}[u,z]$:

$$\bar{F}(z,u) = \bar{F}_1\bar{F}_2\ldots\bar{F}_k.$$

The polynomials $\bar{F}_1\ldots\bar{F}_k$, may be reducible. The permutations in G fix F_1, and so $\bar{F}_1$. The other permutations of the u's map $\bar{F}_1$ into $\bar{F}_2,\ldots,\bar{F}_k$. The permutations in $\bar{G}$ map an irreducible factor of $\bar{F}_1$ into itself so that they cannot map $\bar{F}_1$ into $\bar{F}_2,\ldots,\bar{F}_k$, but must map $\bar{F}_1$ into $\bar{F}_1$, which means that $\bar{G} \subset G$. □

The theorem is frequently used for determining the group G. In particular, we often choose the ideal $\mathfrak{p}$ in such a manner that the polynomial $f(x)$ factors mod $\mathfrak{p}$, since in this way we can narrow down the list of candidates for $\mathrm{Gal}(f)$. For example, let $f(x)$ factor mod$\mathfrak{p}$ so that

$$f(x) \equiv \phi_1(x)\phi_2(x)\ldots\phi_h(x) \pmod{\mathfrak{p}}.$$

It follows that

$$\bar{f} = \bar{\phi}_1\bar{\phi}_2\ldots\bar{\phi}_h.$$

The Galois group $\bar{G}$ of $\bar{f}(x)$ is always cyclic. In fact, the automorphism group of a finite field is always cyclic, as explained in Appendix B. Let the generating permutation s of $\bar{G}$ be

$$(1\,2\ldots j)(j+1\ldots)\ldots.$$

Since the transitivity sets of the group $\bar{G}$ correspons exactly to the irreducible factors of $\bar{f}$, the numbers occurring in the cycles $(12\ldots j)(\ldots)\ldots$ must exacly denote the roots of $\bar{\phi}_1$, $\bar{\phi}_2, \dots \bar{\phi}_h$. Thus, as soon as the degrees $j, k, \dots$ of $\phi_1, \phi_2, \dots$ are known, the type of the substitution s is known as well: s consists of a cycle of j terms, of a cycle of k terms, and so on. Since, with a suitable arrangement of the roots, $\bar{G} \subset G$ by Lemma 2.2.2, G must contain a permutation of the same type.

Example 2.2.3. *Let $f(x) = x^4 - x^3 + x^2 - x + 1 \in \mathbb{Z}[x]$. Since $f(x) = \Phi_{10}(x)$, it resolves modulo $p = 19$ into 2 irreducible factor of the second degree, that is $\bar{f} \equiv (x^2 + 4x + 1) \cdot (x^2 + 14x + 1) \pmod{19}$. Therefore the Galois group $\mathrm{Gal}(f)$ contains a permutation with cycle pattern $2^2 = (--)(--)$.*

We give the following as a corollary of Lemma 2.2.2, even if it is currently referred to as a theorem.

Corollary 2.2.4 (Dedekind's Theorem). *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree m, and let p be a prime number such that $f \bmod p$ has simple roots, that is $p \nmid \Delta(f)$. Suppose that $\bar{f} = \prod f_i$ with f_i irreducible of degree m_i in $\mathbb{F}_p[x]$. Then $\mathrm{Gal}(f)$ contains an element whose cycle decomposition is of the type $m = m_1 + \cdots + m_r$.*

The above result gives the following strategy for computing the Galois group of an irreducible polynomial $f \in \mathbb{Z}[x]$. Factor f modulo a sequence of primes p not dividing $\Delta(f)$ to determine the cycle types of the elements in G_f; continue until a sequence of prime numbers has yielded no new cycle types for the elements. Then attempt to read off the type of the group from tables of transitive groups of degree ∂f. To make the computation more effective, in the technical sense, we need the *Frobenius Theorem.*

2.3 Frobenius's Theorem

The theorem of Frobenius $(1849 - 1917)$ that Chebotarëv generalized deserves to be better known than it is. For many applications of Chebotarëv's theorem it suffices to have Frobenius's theorem, which is both older (1880) and easier to prove than Chebotarëv's theorem (1922). Again, Frobenius's theorem can be discovered empirically. Consider a polynomial with integer coefficients, say $f(x) = x^4 - x^3 + x^2 - x + 2$, and suppose that one is interested in deciding whether or not $f(x)$ is irreducible over the ring $\mathbb{Z}$ of integer. A standard approach is to factor $f(x)$ modulo several prime numbers p: if the leading coefficient of f is not divisible by p, then a nontrivial factorization $f = gh$ in $\mathbb{Z}[x]$ will give a nontrivial factorization $\bar{f} = \bar{g}\bar{h}$ in $\mathbb{F}_p[x]$. Thus, if $f(x)$ is irreducible in $\mathbb{F}_p[x]$ for some prime p not dividing its leading coefficient, then it is irreducible in $\mathbb{Z}[x]$. This test is very useful, but it is not always effective: in [Bra86], the author proves that every non–prime integer $n \geq 1$ occurs as the degree of a polynomial in $\mathbb{Z}[x]$ that is irreducible over $\mathbb{Z}$ but reducible modulo all primes.

According to Maple, we have

$$f(x) \equiv (x+1)(x^3 + x^2 + 2) \pmod{3}.$$

We say that the decomposition type of (f mod 11) is 1, 3. It follows that if $f(x)$ is reducible over $\mathbb{Z}$, then its decomposition type will likewise be 1, 3: a product of a linear factor and a factor of degree 3. However, the latter alternative is incompatible with the fact that the decomposition type modulo 5 is 2, 2:

$$f \equiv (x^2 + 2x + 4)(x^2 + 2x + 3) \pmod{5},$$

where the two factors are irreducible over $\mathbb{F}_5$. One concludes that f is irreducible over $\mathbb{Z}$.

Could the irreducibility of $f(x)$ have been proven with a single prime? Modulo such a prime number, $f(x)$ would have to be irreducible, with decomposition type equal to the single number 4. Maple make it easy to do numerical experiments. There are 168 prime numbers below 1000. Two of these, $p = 2$ and $p = 349$, are special, in the sense that f acquires repeated factors modulo p: $f(x) \equiv x(x+1)^3 \pmod{2}$ and $f \equiv (x+177)^2(x^2 + 343x + 112) \pmod{349}$. Indeed 2 and 349 divide $\Delta(f)$ For no other prime does this happen, and the following types are found.

It is suggested that the primes with type 1, 1, 1, 1 have density $\frac{1}{12}$; the primes with type 4 and 1, 1, 2 have desity $\frac{1}{4}$; the primes with type 1, 3 have

Type 1, 1, 1, 1:	6	primes (4%),
Type 1, 1, 2:	42	primes (25.5%),
Type 2, 2:	21	primes (12.5%),
Type 1, 3:	51	primes (31%),
Type 4:	46	primes (27%).

density $\frac{1}{3}$; finally, to make the densities add up to 1, the primes with type 2, 2 have density $\frac{1}{8}$. Frobenius's theorem tells how to understand these fractions through the Galois group of the polynomial.

Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial, and denote the degree of $f(x)$ by n. Assume that the discrimmant $\Delta(f)$ does not vanish, so that $f(x)$ has n distinct zeros $\alpha_1, \alpha_2, \cdots, \alpha_n$ in a suitable extension field of the field $\mathbb{Q}$. Write K for the field generated by these zeros, $K = \mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_n)$. The Galois group G of $f(x)$ is the group of field automorphisms of K. Each $\sigma \in G$ permutes the zeros $\alpha_1, \alpha_2, \cdots, \alpha_n$ of f, and is completely determined by the way in which it permutes these zeros. Hence, we may consider G as a subgroup of the group S_n of permutations of n symbols. Writing an element $\sigma \in G$ as a product of disjoint cycles, including cycles of length 1, and looking at the lengths of these cycles, we obtain the cycle pattern of σ, which is a partition of n. If p is a prime number not dividing $\Delta(f)$, then we can write $f \pmod{p}$ as a product of distinct irreducible factors over $\mathbb{F}_p$. The degrees of these irreducible factors form the decomposition type of f modulo p; this is also a partition of n. Frobenius's theorem asserts, roughly speaking, that the number of prime numbers p with a given decomposition type is proportional to the number of $\sigma \in G$ with the same cycle pattern. So we have the following.

Theorem 2.3.1 (Frobenius's Theorem). *The density of the set of prime p for which f mod p has a given decomposition type $n_1, n_2, \cdots, n_i$, exists, and it is equal to $1/\#\mathrm{Gal}(f)$ times the number of $\sigma \in G$ with decomposition in disjoint cycle of the form $c_{n_1} c_{n_2} \cdots c_{n_i}$, where c_{n_k} is a n_k–cycle.*

Let us consider the partition in which all n_i are equal to 1. Only the identity permutation has this cycle pattern. Hence the set of primes p for which f modulo p splits completely into linear factors has density $1/\#G$.

2.4 Chebotarëv's Theorem

To introduce Chebotarëv's theorem we need the theory of Dedekind's Domains explained in Section 1.5.
For any prime ideal $\mathfrak{p}$ of K unramified in L, the Frobenius element

$$(\mathfrak{p}, L/K) = \{(\mathfrak{P}, L/K) s.t. \mathfrak{P} \mid \mathfrak{p}\}$$

is a conjugacy class in G. Given an element of $\mathrm{Gal}(L/K)$, can it be represented as a Frobenius element of a prime ideal? This question and more is answered by the following.

Theorem 2.4.1 (Chebotarëv's Density Theorem). *Let L be a Galois extension of number field K, and for $\sigma \in \mathrm{Gal}(L/K)$ define C_σ to be the conjugacy class of σ. Let S be the set of unramified prime ideals $\mathfrak{p}$ of K such that for every prime ideal $\mathfrak{P}$ of L dividing $\mathfrak{p}$, the Frobenius element of $\mathfrak{P}$ is C_σ. Then S has Dirichlet density*

$$\frac{\#C_\sigma}{\#\mathrm{Gal}(L/K)}.$$

If S is a set of primes of K, then we define the analytic density of S to be

$$\delta_{an}(S) = \lim_{x\to\infty} \frac{\#\{\mathfrak{p} : \#(\mathcal{O}_k/\mathfrak{p}) \leq x, \mathfrak{p} \in S\}}{\#\{\mathfrak{p} : \#(\mathcal{O}_k/\mathfrak{p}) \leq x, \mathfrak{p}\, prime\}}$$

if this limit exists. If the analytic density exists, then it is actually equal to the Dirichlet density

$$\delta_{an}(S) = \lim_{s\to 1^+} \left(\sum_{\mathfrak{p}\in S} \frac{1}{\#(\mathcal{O}_K/\mathfrak{p})^s}\right)\left(\sum_{\mathfrak{p}\, prime} \frac{1}{\#(\mathcal{O}_K/\mathfrak{p})^s}\right)^{-1}.$$

The converse is not true: there are cases where the Dirichlet density exists but the analytic one does not. However, the Chebotarëv Density Theorem is valid with either notion of density.

2.5 Frobenius and Chebotarëv

In the last section we said that Chebotarëv generalized Frobenius's theorem. In order to explain it clearly, let us consider the following reformulation.

Theorem 2.5.1 (Chebotarëv's Density Theorem). *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial. Assume that the discriminant $\Delta(f)$ of $f(x)$ does not vanish. Let C be a conjugacy class of the Galois group G of $f(x)$. Then the set of primes p not dividing $\Delta(f)$ for which σ_p belongs to C has a density, and this density equals $|C|/|G|$.*

On first inspection, one might feel that Chebotarëv's theorem is not much stronger than Frobenius's version. In fact, applying the latter to a well–chosen polynomial, with the same splitting field of $f(x)$, one finds a variant of the density theorem in which C is required to be a *division* of G rather than a conjugacy class; here we say that two elements of G belong to the same if the cyclic subgroups that they generate are conjugate in G. Frobenius himself reformulated his theorem already in this way. The partition of G into divisions is, in general, less fine than its partition into conjugacy classes and Frobenius's theorem is correspondingly weaker than Chebotarëv's.
Let $\sigma = (1\,2\,3\,4)$ be such that the cyclic group is $C_4 = \langle\sigma\rangle$. Table 2.1 shows the difference between these partitions.

Conjugacy classes of C_4	$\{id\}$	$\{\sigma\}$	$\{\sigma^3\}$	$\{\sigma^2\}$
Divisions of C_4	$\{id\}$	$\{\sigma, \sigma^3\}$		$\{\sigma^2\}$

Table 2.1: Partition of C_4 into divisions and conjugacy classes.

Applying Frobenius's and Chebotarëv's theorem to the 10–th cyclotomic polynomial $\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$, which has Galois group C_4, we get the distributions shown in Table 2.2.

We computed Table 2.2 just considering primes $p \leq 1000$. In particular, from the second line in Table 2.2 we get the cycle distribution of $\mathrm{Gal}(f)$ and

C_4	$\{id\}$	$\{\sigma\}$	$\{\sigma^3\}$	$\{\sigma^2\}$	C_4	$\{id\}$	$\{\sigma, \sigma^3\}$	$\{\sigma^2\}$
Chebotarëv	$\frac{5}{21}$	$\frac{19}{84}$	$\frac{47}{168}$	$\frac{1}{4}$	Frobenius	$\frac{40}{167}$	$\frac{89}{167}$	$\frac{38}{167}$

Table 2.2: Chebotarëv's and Frobenius's informations.

from these datas we conclude that $\mathrm{Gal}(f) \simeq C_4$. Increasing the range, the distributions will be closer to the theoretical results given in Table 2.3.

C_4	$\{id\}$	$\{\sigma\}$	$\{\sigma^3\}$	$\{\sigma^2\}$	C_4	$\{id\}$	$\{\sigma, \sigma^3\}$	$\{\sigma^2\}$
Chebotarëv	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	Frobenius	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$

Table 2.3: Theoretical informations.

2.6 Dirichlet's Theorem on Primes in Arithmetic Progression

Chebotarëv's density theorem may be regarded as the least common generalization of Dirichlet's theorem on primes in arithmetic progressions (1837) and Frobenius's theorem (1880; published 1896). Dirichlet's theorem is easy to discover experimentally. Here are the prime numbers below 100, arranged by final digit:

- 1 : 11; 31; 41; 61; 71
- 2 : 2
- 3 : 3; 13; 23; 43; 53; 73; 83
- 5 : 5
- 7 : 7; 17; 37; 47; 67; 97
- 9 : 19; 29; 59; 79; 89

It does not come as a surprise that no prime numbers end in $0, 4, 6,$ or 8, and that only two prime numbers end in 2 or 5. The table suggests that there are infinitely many primes ending in each of $1, 3, 7, 9$, and that, approximately, they keep up with each other. This is indeed true; it is the special case $m = 10$ of the following theorem, proved by Dirichlet in 1837. Write $\varphi(m)$ for the Euler function evaluated in m. Our goal is to prove the following.

Theorem 2.6.1 (Dirichlet's Theorem). *Let m be a positive integer. Then for each integer a with $\gcd(a, m) = 1$ the set S of prime numbers p such that $p \equiv a \pmod{m}$ has density $1/\varphi(m)$.*

Hence we will show that there are "equally many" prime numbers $p \equiv a \pmod{m}$ for each $a \in (\mathbb{Z}/m\mathbb{Z})^*$.
To see how Dirichlet's theorem follows, let $K = \mathbb{Q}$ and let $L = \mathbb{Q}(\zeta_m)$, where ζ_m is one of the primitive m–th roots of unity. $\mathbb{Q}(\zeta_m)$ is an abelian extension of $\mathbb{Q}$ and we can identify its Galois group with $(\mathbb{Z}/m\mathbb{Z})^*$; so $C_\sigma = \{\sigma\}$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, and the Frobenius element of $\mathfrak{P}$ is just

$$(\mathfrak{p}, \mathbb{Q}(\zeta_m)/\mathbb{Q}) = p \pmod{m} \in (\mathbb{Z}/m\mathbb{Z})^*$$

for all $\mathfrak{P}$ dividing any prime number $p \nmid m$, as explained in Example 1.6.8. Thus we see that there is a bijective correspondence between the conjugacy classes $\pmod{m}$ of prime numbers that do not divide m and the elements of the Galois group, so that the set S in the statement of the theorem becomes $S_a = \{\text{prime numbers } p \in \mathbb{Z} \text{ s.t. } p \equiv a \pmod{m}\}$. Since $\#C_\sigma = 1$ and $\#\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \varphi(m)$, the theorem tells us that the set S_a has density $1/\varphi(m)$ for each $a \in (\mathbb{Z}/m\mathbb{Z})^*$, which is exactly Dirichlet's theorem.
We can follow the same strategy using Frobenius's theorem, instead of Chebotarëv's. However, this choice does not work for all m.

Example 2.6.2. *Case $m = 12$. Let $f(x)$ be the polynomial $x^{12} - 1 = (x-1)(x+1)(x^2+1)(x^2+x+1)(x^2-x+1)(x^4-x^2+1)$. According to Theorem 1.2.5, we find that the decomposition type depends only on the residue class of p modulo 12.*

$p \equiv 1$	$\pmod{12}$	$\Rightarrow (1)^{12}$
$p \equiv 5$	$\pmod{12}$	$\Rightarrow (1)^4,\ (2)^4$
$p \equiv 7$	$\pmod{12}$	$\Rightarrow (1)^6,\ (2)^3$
$p \equiv 11$	$\pmod{12}$	$\Rightarrow (1)^2,\ (2)^5$

Table 2.4: Decomposition types of $f(x) = x^{12} - 1$ modulo different primes.

Looking at Table 2.4 we conclude that Frobenius's theorem implies Dirichlet's theorem in the case $m = 12$*, since the four decomposition type are pairwise distinct.*
Let us consider now the case $m = 8$*. Let* $f(x)$ *be the polynomial* $x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1)$*. According to Theorem 1.2.5, we find that the decomposition type depend only on the residue class of* p *modulo* 8*.*

$p \equiv 1$	$\pmod{8}$	$\Rightarrow (1)^8$
$p \equiv 5$	$\pmod{8}$	$\Rightarrow (1)^4,\ (2)^2$
$p \equiv 7$	$\pmod{8}$	$\Rightarrow (1)^2,\ (2)^3$
$p \equiv 11$	$\pmod{8}$	$\Rightarrow (1)^2,\ (2)^3$

Table 2.5: Decomposition types of $f(x) = x^8 - 1$ modulo different primes.

However, in this case Frobenius's Theorem does not distinguish between the residue class $7 \bmod 8$ *and* $11 \bmod 8$*, since these classes belong to the same division. Dirichlet's theorem is not implied in this case and we need to use the stronger statement of the Chebotarëv density theorem.*

It's interesting to observe that although Theorem 2.6.1 involves only integers, its simplest proof requires the use of complex numbers and Dirichlet L–series. The proof of the Chebotarëv density theorem is a generalization of that one of Dirichlet's theorem. Here we illustrate how Dirichlet implies Chebotarëv in the case of quadratic extensions.
Let $L = \mathbb{Q}(\sqrt{m})$, with m square–free, and $K = \mathbb{Q}$, so that the Galois group of this extension must be the group with two elements, namely $\mathbb{Z}/2\mathbb{Z}$. Since

this group is abelian, every element has only one conjugate. Thus, viewing the Galois group as an multiplicative group, the primes with Frobenius element 1 must have density 1/2, as should the primes with Frobenius element -1. Now, from the definition of the Frobenius element, we know that, in this case, primes that remain prime in $\mathcal{O}_L$ should correspond to a Frobenius element of order 2, and primes that split into two primes in $\mathcal{O}_L$ should correspond to a Frobenius element of order 1; this results from the fact that the order of the Frobenius element is $f = f(\mathfrak{P}/\mathfrak{p})$, the relative degree of $\mathfrak{p}$. Thus, what Chebotarëv's theorem states in this case is that the density of the set of primes that split and the density of primes that remain prime in O_L is 1/2. In Example 1.6.11 we have seen that there is a simple way to characterize each of these sets: $\mathfrak{p} = p\mathbb{Z}$ remains prime in $\mathcal{O}_L$ if and only if m is not a square modulo p.

Our statement becomes: the density of primes p such that a given square–free integer m is a square $\bmod p$ is 1/2. In the following arguments, we might be concerned about the case where $p \mid m$. We have actually already thrown out these cases by discarding ramified primes. From Theorem 1.5.9 we know that such primes are exactly those which divide the discriminant and, in this case, the discriminant is divisible by m. Now we are ready to use Dirichlet's theorem on primes in arithmetic progressions to prove the following.

Proposition 2.6.3. *For a quadratic extention $\mathbb{Q}(\sqrt{m})$, Dirichlet's theorem implies Cheboterev's theorem.*

Proof. First, consider $\left(\frac{p}{q}\right)$ where q is an odd prime. If $q \equiv 1 \bmod 4$, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ for all p. Since half the residues modulo any integer are squares, this gives us our result in the case where $q \equiv 1 \bmod 4$, since exactly $\varphi(q)/2$ residues are squares modulo q and the density of the set of primes congruent to each residue is $1/\varphi(q)$, so the density of primes which are squares modulo q is

$$\frac{\varphi(q)}{2}\frac{1}{\varphi(q)} = \frac{1}{2},$$

and the primes that are squares modulo q are exactly the primes for which

q is a square.

The other case, $q \equiv 3 \bmod 4$, is more difficult. If $p \equiv 1 \bmod 4$, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, but if $p \equiv 3 \bmod 4$, $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$. To deal with this, consider Dirichlet's theorem applied to $4q$. This tells us that the density of the primes in each equivalence class of $(\mathbb{Z}/(4q)\mathbb{Z})^*$ is $1/\varphi(4q)$. The Chinese remainder theorem says that exactly half these equivalence classes contain the primes congruent to 1 mod 4. Thus, if we consider only the set of primes congruent to 1 mod 4, the primes in this set congruent to a given $a \in (\mathbb{Z}/q\mathbb{Z})^*$ must have density $1/\varphi(q)$. For primes in this set, $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, so the density of primes in this set for which q is a square must be $1/2$. Considering the set of primes congruent to 3 mod 4, the fact that the density of primes in this set which are not squares modulo q must be $1/2$ gives us the same result. Thus the density of all primes for which q is a square must be $1/2$.

Now, if we let $m = q_1 q_2 \cdots q_n$ where all the q_i are distinct, we can obtain the same result if we consider that the primes congruent to 1 mod 4 are equally distributed over $\mathbb{Z}/m\mathbb{Z}$ and that for primes p in this set,

$$\left(\frac{q_1 q_2 \cdots q_{n-1}}{p}\right)$$

is completely determined by the residue of $p \bmod (q_1 q_2 \cdots q_{n-1})$. Then if we consider the subset A of these primes congruent to a given $a \bmod (q_1 q_2 \cdots q_{n-1})$, the subset of primes in A congruent to a given $b \bmod (q_n)$ must have density $\varphi(q_n)$ in A. Then

$$\left(\frac{m}{p}\right) = \left(\frac{q_1 q_2 \cdots q_{n-1}}{p}\right)\left(\frac{q_n}{p}\right).$$

For primes in A, the former factor is constant, and the set of primes for which the latter factor is 1 has density $1/2$. Thus m is a square modulo p for half the primes in A. Since a was arbitrary, the density of primes congruent to 1 mod 4 for which m is a square must be $1/2$. A similar argument applies for the primes congruent to 3 mod 4, so we achieve our result in general: the density of primes for which a given m is a square is $1/2$. □

2.7 Hint of the Proof

In this section we give a proof of Chebotarëv's theorem that follows his original strategy, not including class field theory. We refer to [SL96] for more details.

Let L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K)$. For all primes $\mathfrak{p}$ not containing the discriminant ideal $(\Delta(L/K))$ there exists a Frobenius element $\sigma_{\mathfrak{p}}$, which is an element of G well defined up to conjugacy.

Theorem 2.7.1 (Chebotarëv's theorem). *For any conjugacy class C of G, the density $d(L/K, C)$ of the set $S = \{\mathfrak{p} \in K \text{ s.t. } \sigma_{\mathfrak{p}} \in C\}$ exists and equals $\#C/\#G$.*

Proof. The first step in our proof is the reduction to the abelian case. Let $\sigma \in C$ and $E = \{x \in L \text{ s.t. } \sigma x = x\}$. Then L is a Galois extension of E with $\mathrm{Gal}(L/E) = \langle\sigma\rangle$. Chapter 8 of [Lan94] shows that the conclusion of the theorem holds for L, K, C if and only if it holds for L, E, $\{\sigma\}$. Note that $\mathrm{Gal}(L/E)$ is abelian, since $E = L^{\langle\sigma\rangle}$. Next one considers the case that L is cyclotomic over K and proves the theorem in this case, as explained in [SL96].

With this tools we are able to approach a general proof. We assume L/K to be an abelian extension of degree n, with $G = \mathrm{Gal}(L/K)$. Let $m\mathcal{O}_K$ be a prime not ramified, and $\zeta = \zeta_m$. Then $H = \mathrm{Gal}(K(\zeta)/K) \simeq (\mathbb{Z}/m\mathbb{Z})^*$ and $\mathrm{Gal}(L(\zeta)/K) \simeq G \times H$. If a prime $\mathfrak{p}$ of K has Frobenius element (σ, τ) in $G \times H$, then it has Frobenius element σ in G. Hence $\delta_{inf}(L/K, \{\sigma\}) \geq \sum_{\tau\in H} \delta_{inf}(L(\zeta)/K, \{(\sigma, \tau)\})$. If we fix σ and τ, and suppose that n divides $ord_H(\tau)$, then $\langle(\sigma, \tau)\rangle \cap G \times \{1\}$ is the trivial group, and therefore, $M = L^{\langle(\sigma,\tau)\rangle}$ satisfies $M(\zeta) = L(\zeta)$. So $L(\zeta)/M$ is a cyclotomic extension. But we have assumed that in this case the theorem holds, i.e. $\delta\{L(\zeta)/M, (\sigma, \tau)\}$ exists and has the correct value; then the same holds for $\delta\{L(\zeta)/K, (\sigma, \tau)\}$, which equals $1/(\#G{\cdot}\#H)$. Let $H_n = \{\tau \in H \text{ s.t. } n|\mathrm{ord}_H(\tau)\}$; then $\delta_{inf}(L/K), \{\sigma\} \geq \sum_{\tau\in H} 1/(\#G \cdot \#H) = \#H_n/(\#G \cdot \#H)$. When m ranges over all primes not ramified in L, the fraction $\#H_n/\#H$ gets arbitrarily close to 1, so that

$\delta_{inf}(L/K) \geq 1/\#G$. Applying this to all other elements of the group one finds that $\delta_{sup}(L/K, \{\sigma\}) \leq 1/\#G$; hence $\delta(L/K, \{\sigma\}) = 1/\#G$. $\square$

Chapter 3

Applications

3.1 Charming Consequences

First, we have an interesting result about primes p for which $(f \bmod p)$ has no zeros. For the following we refer to [Ser03].

Theorem 3.1.1. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree $n > 1$. If p is prime, let $N_p(f)$ be the number of zeros of f in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Then there are infinitely many p's such that $N_p(f) = 0$. Moreover the set $P_0(f)$ of p's with $N_p(f) = 0$ has a density $c_0 = c_0(f) \geq 1/n$.*

To prove the statement above we will use the Burneside Lemma, for which we refer to [Rot95].

Notation 3.1.2. *If φ is a function on G, and $S \subset G$, we denote by $\int_S \varphi$ the number $\frac{1}{|G|}\sum_{g\in S}\varphi(g)$. When $S = G$, we write $\int \varphi$ instead of $\int_G \varphi$.*

Lemma 3.1.3 (Burniside's Lemma). *If X is a finite G–set and $\chi(g)$ is the number of fixed points of g on X, then the number of G–orbits of X is equal to*

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \int \chi.$$

Proof. In $\sum_{g\in G}\chi(g)$, each $x \in X$ is counted $|Stab_G(x)|$ times. If x and y lie in the same orbit, then $|Stab_G(x)| = |Stab_G(y)|$ because they are conjugated in

G. So the $(G : Stab_G(x))$ elements constituing the orbit of x are collectively counted $(G : Stab_G(x))|Stab_G(x)|$ times. Each orbit thus contributes $|G|$ to the sum, and so we have $\frac{1}{|G|}\sum_{g\in G}\chi(g)$ orbits. □

Corollary 3.1.4. *If X is a finite transitive G–set with $|X| > 1$, then there exists $g \in G$ having no fixed points.*

Proof. Since the action of G on X is transitive, the number of G–orbits is 1, and so Burnside's Lemma gives

$$1 = \frac{1}{|G|}\sum_{g\in G}\chi(g).$$

Now $\chi(1) = |X| > 1$. If $\chi(g) \geq 1$ for every $g \in G$, then the right hand side is too large. □

We are ready to prove Theorem 3.1.1.

Proof. Let $\chi^2(g)$ be the number of points of $X \times X$ fixed by $g \in G$ and $\int \chi^2$ be the number of orbits of G on $X \times X$. Then is $\int \chi^2 \geq 2$, as one sees by decomposing $X \times X$ into the diagonal and its complement. We will denote with G_0 the set of $g \in G$ with $\chi(g) = 0$. If $g \notin G_0$, we have $1 \leq \chi(g) \leq n$ and therefore

$$(\chi(g) - 1)(\chi(g) - n) \leq 0.$$

Hence

$$\int_{G-G_0}(\chi(g) - 1)(\chi(g) - n) \leq 0,$$

that is

$$\int_G(\chi(g) - 1)(\chi(g) - n) \leq \int_{G_0}(\chi(g) - 1)(\chi(g) - n) \leq n\int_{G_0} 1.$$

The left hand side is

$$\int_G(\chi^2 - (n + 1)\chi + n),$$

while the right hand side is

$$n\int_{G_0} 1 = n\frac{1}{|G|}\sum_{g\in G_0} 1 = n\frac{|G_0|}{|G|} = nc_0.$$

Finally, $\int \chi = 1$, since the action is transitive. From Lemma 3.1.3 we have

$$\int_G (\chi^2 - (n+1)\chi + n) \geq 2 - (n+1) + n = 1,$$

hence $1 \leq nc_0$. To conclude our proof, we use Chebotarëv's Density Theorem. Let $f(x) \in \mathbb{Z}[x]$ be the polynomial in the statement and $X = \{\alpha_1, \dots, \alpha_n\}$ be the set of its distinct roots. We know that $G = \mathrm{Gal}(f)$ acts transitively on X. Now, we denote with G_0 the set $\sigma \in G$ with no fixed points; from the above result, $|G_0|/|G| \geq 1/n$. The key–observation is that $N_p(f) = 0 \Leftrightarrow \sigma_p \in G_0$, since the decomposition type of $(f \bmod p)$ equals the cycle pattern of the Frobenius element $\sigma = \sigma_p \in G$, and so every fixed point of σ_p corresponds to a linear factor, i.e. to a root, of $(f \bmod p)$. Moreover, G_0 is stable under conjugation so that, from Theorem 2.5.1, the set $\{p \text{ s.t. } \sigma_p \in G_0\}$ has density $c_0 = |G_0|/|G| \geq \frac{1}{n}$. Thus there are infinitely many p's such that $N_p(f) = 0$ □

Note also that Burnside's Lemma, combined with Chebotarëv's Density Theorem, gives the following result, due to Kronecker.

Theorem 3.1.5. *Let f be as in Theorem 3.1.1. Then the mean value of $N_p(f)$ for $p \to \infty$ is equal to* 1.

In fact, if G acts transitively on X, then from Lemma 3.1.3 we have

$$1 = \frac{1}{|G|} \sum_{g \in G} \chi(g),$$

so that the mean value of $\chi(g)$ is 1, for each $g \in G$. But each $g \in G$ can be seen as the Frobenius element σ_p, for some p, whose cycle pattern equals the decomposition type of $(f \bmod p)$. Therefore the mean value of zeros of $(f \bmod p)$ is 1.
In other words,

$$\sum_{p \leq x} N_p(f) \approx \pi(x) \text{ when } x \to \infty.$$

It's very easy to test this formula for any irreducible polynomial f if we know the cycle type distribution of it's Galois group.

Example 3.1.6. *Let $f(x) = x^3 - 2$ so that* $\mathrm{Gal}(f) \simeq S_3$. *Knowledge of cycle pattern in* $\mathrm{Gal}(f)$ *allows us to figure out the number of roots modulo each prime number: they corresponds to the number of fixed point of each permutation, as explained in Table 3.1.*
According to the above result, the mean value of $N_p(f)$ is 1. We can prove this computing

$$\sum(\textit{Fixed points}) \cdot (\textit{Distribution}),$$

where the sum is extended to all cycle type in S_3. Hence

$$\frac{\sum_p N_p(f)}{\sum_p 1} = 3 \cdot 1/6 + 1 \cdot 1/2 = 1$$

as the theoretical result predicts.

Cycle type	$(-)$	$(--)$	$(---)$
Distribution	$\frac{1}{6}$	$\frac{1}{2}$	$\frac{1}{3}$
Fixed points	3	1	0

Table 3.1: Distribution and fixed points of cycle type in S_3.

In Section 2.3 we said that it's always possible to construct an irreducible polynomial of non–prime degree which is reducible modulo all primes. What we can state about polynomial that have a root, that is, a linear factor, modulo all primes? With a little group theory, we can get our answer to this question. This result can be found in the article [LS91] by Lenstra and Stevenhagen.

Theorem 3.1.7. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial that has a zero modulo almost all primes p. Then $f(x)$ is linear.*

Proof. Assume that $\partial f > 1$, and let G be the Galois group of the splitting field of f. Then G acts transitively on the set Ω of roots of f, and the assumption that f has a root modulo p for almost all p implies that almost all Frobenius elements in G fix a root of f. If $H \subset G$ is the stabilizer of some $\omega \in \Omega$, the subset of G consisting of those elements that fix at least one element of Ω equals $\bigcup_{g \in G} gHg^{-1}$, because we have a transitive action and $Stab_G(g\omega) = gStab_G(\omega)g^{-1}$. From Corollary 3.1.4, G contains at least an element that fix no root of f, and which therefore occurs as the Frobenius of only finitely many primes in the splitting field of f. This obviously contradicts the Chebotarëv density theorem. $\square$

3.2 Primes and Quadratic Forms

For the theory developed in this section we refer to [Cox89]. We will prove the classical theorem that a primitive positive definite quadratic form $ax^2 + bxy + cy^2$ represents infinitely many prime numbers. We will just consider particular cases, since a general proof should involve Class Field Theory.
A first definition is the following.

Definition 3.2.1. *A form $f(x, y) = ax^2 + bxy + cy^2$ is primitive if a, b, c are relatively prime.*

We will deal exclusively with primitive forms. An integer m is represented by a form $f(x, y)$ if the equation $m = f(x, y)$ has integer solution in x and y; if $\gcd(x, y) = 1$, then we say that m is properly represented by $f(x, y)$.
Next, we say that $f(x, y)$ and $g(x, y)$ are *equivalent* if there are integers p, q, r, s such that

$$f(x, y) = g(px + qy, rx + sy) \text{ and } ps - qr = \pm 1.$$

An important observation is that equivalent forms properly represent the same numbers. Then we say that an equivalence is a *proper equivalence* if $ps - qr = 1$, and it is an *improper equivalence* if $ps - qr = -1$.
There is a very nice relation between proper representation and proper equivalence.

Lemma 3.2.2. *A form $f(x, y)$ properly represents an integer m if and only if $f(x, y)$ is properly equivalent to the form $mx^2+bxy+cy^2$, for some $b, c \in \mathbb{Z}$.*

Proof. ($\Rightarrow$) suppose that $m = f(p,q)$, with $\gcd(p,q) = 1$. We can find r and s so that $ps - qr = 1$, and then

$$\begin{aligned} f(px+ry, qx+sy) &= f(p,q)x^2 + (2apr + bps + brq + 2cqs)xy + f(r,s)y^2 \\ &= mx^2 + bxy + cy^2. \end{aligned}$$

($\Leftarrow$) Note that $mx^2 + bxy + cy^2$ represents properly m taking $(x,y) = (1,0)$. □

We define the discriminant of $ax^2+bxy+cy^2$ to be $D = b^2-4ac$; equivalent forms have the same dicriminant. We will consider only positive definite forms, that is, forms such that $a > 0$ and $D < 0$.
We have the following necessary and sufficient condition for a number m to be represented by a form of discriminant D.

Lemma 3.2.3. *Let $D \equiv 0, 1 \bmod 4$ be an integer and m be an odd prime with $\gcd(D,m) = 1$. Then m is properly represented by a primitive form of discriminant D if and only if $\left(\frac{D}{m}\right) = 1$.*

Proof. ($\Rightarrow$) From lemma 3.2.2 we may assume $f(x,y) = mx^2 + bxy + cy^2$, since $f(x,y)$ properly represents m. Thus $D = b^2 - 4mc \equiv b^2 \bmod m$.
($\Leftarrow$) Suppose that $D \equiv b^2 \bmod m$. Since m is odd, we may assume that D and b have the same parity, replacing b by $b+m$ if necessary. Then $D \equiv 0, 1 \bmod 4$ implies $D \equiv b^2 \bmod 4m$. This means that $D = b^2 - 4mc$ for some c. Then $mx^2+bxy+cy^2$ represents m properly and has discriminant D, and the coefficients are relatively prime since m is relatively prime to D. □

Corollary 3.2.4. *Let n be an integer and let p be an odd prime not dividing n. Then $\left(\frac{-n}{p}\right) = 1$ if and only if p is represented by a primitive form of discriminant $-4n$.*

Proof. From Lemma 3.2.3, $-4n$ is a quadratic residue modulo p if and only if $\left(\frac{-4n}{p}\right) = \left(\frac{-n}{p}\right) = 1$. □

A primitive positive definite form $ax^2 + bxy + cy^2$ is said to be reduced if

$$|b| \leq a \leq c, \text{ and } b \geq 0 \text{ if either } |b| = a \text{ or } a = c.$$

The basic theorem is the following, which we give without proof.

Theorem 3.2.5. *Every primitive positive definite form is properly equivalent a unique reduced form. Moreover, the number $h(D)$ of classes of primitive positive definite forms of discriminant D is finite, and $h(D)$ is equal to the number of reduced forms of discriminant D.*

D	$h(D)$	Reduced forms of discriminant D
-4	1	$x^2 + y^2$
-8	1	$x^2 + 2y^2$
-12	1	$x^2 + 3y^2$
-20	2	$x^2 + 5y^2$, $2x^2 + 2xy + 3y^2$
-28	1	$x^2 + 7y^2$

Table 3.2: Computation of $h(-4n)$ for $n = 1, 2, 3, 5, 7$.

The crucial observation is that there exist a natural isomorphism between the ideal class group $\mathcal{C}l(\mathcal{O}_K)$ and the class group of primitive positive definite forms of discriminant D. For example, in the case of quadratic fields, the isomorphism is given by the map

$$ax^2 + bxy + cy^2 \mapsto [a, (-b + \sqrt{\Delta(\mathcal{O}_K/\mathbb{Z})})/2].$$

In the following we show how to use these notions to get information on primes represented by a quadratic form.

Example 3.2.6. *Case $D = -4$. We put $f(x) = x^2 + 1$, so that $D(f) = -4$ and its splitting field is $K = \mathbb{Q}(i)$. Obviously $K = \mathbb{Q}(\zeta_4)$ and the ring of integers $\mathcal{O}_K$ equals $\mathbb{Z}(\zeta_4)$, which is the ordinary ring of Gauss integer $\mathbb{Z}(i)$. By Lemma 3.2.3 we have that an odd prime p is representable by $x^2 + y^2$ if and only if $\left(\frac{D}{p}\right) = 1$, that is, when $p \equiv 1 \bmod 4$. So we get the famous result by Fermat: the equation $p = x^2 + y^2$ admits integer solutions in (x, y) if and only if $p \equiv 1 \bmod 4$. Furthermore, from Chebotarëv's theorem, the* *density of primes such that* $\left(\frac{D}{p}\right) = 1$ *equals* $1/2$ *and therefore we have the supplementary information*

$$\delta(p \geq 3 \text{ } s.t. \text{ } p = x^2 + y^2) = \frac{1}{2}.$$

By means of analogous investigations in the case $D = -8, -12, -28$ *we get*

$$\begin{array}{llll} \delta(p \text{ } s.t. \left(\frac{-8}{p}\right) = 1) = & \delta(p \geq 3 \text{ } s.t. \text{ } p = x^2 + 2y^2) & = \frac{1}{2} \\ \delta(p \text{ } s.t. \left(\frac{-12}{p}\right) = 1) = & \delta(p \geq 5 \text{ } s.t. \text{ } p = x^2 + 3y^2) & = \frac{1}{2} \\ \delta(p \text{ } s.t. \left(\frac{-28}{p}\right) = 1) = & \delta(p \geq 11 \text{ } s.t. \text{ } p = x^2 + 7y^2) & = \frac{1}{2}. \end{array}$$

The case $D = -20$ is significantly different and more complicated since $h(-20) > 1$ and this fact implies the notion of *ring class field.* A complete explaination of this theory leads us to the following general result.

Theorem 3.2.7. *Let* $ax^2+bxy+cy^2$ *be a primitive positive definite quadratic form of discriminant* $D < 0$*, and let* S *be the set of primes represented by* $ax^2 + bxy + cy^2$*. Then the Dirichlet density* $\delta(S)$ *exists and is given by the formula*

$$\delta(S) = \begin{cases} \frac{1}{2h(D)} & \textit{if } ax^2 + bxy + cy^2 \textit{ is properly equivalent to its opposite,} \\ \frac{1}{h(D)} & \textit{otherwise.} \end{cases}$$

In particular, $ax^2 + bxy + cy^2$ *represents infinitely many prime numbers.*

Therefore, the case $D = -20$ gives the following result:

$$\delta(p = x^2 + 5y^2) = \delta(p = 2x^2 + 2xy + 3y^2) = \frac{1}{2h(D)} = \frac{1}{4}.$$

3.3 A Probabilistic Approach

The Chebotarëv density theorem allows a probabilistic approach to finding G by factoring f modulo different non–ramified primes and cheking for which transitive subgroups of S_n this approximates the shape distribution best. Effective bounds on estimates of these distributions have been calculated by Lagarios and Odlyzko in [LO77] using assumptions based on the

Generalized Riemann Hypothesis, enabling Gal(f) to be determined uniquely in many cases.

In the study of Galois groups of polynomial $f(x)$, we restrict ourselves to monic polynomials with integer coefficients, since any polynomial can easily be transformed into a monic polynomial with integer coefficients equivalent with respect to its Galois group, as explained in the following.

Proposition 3.3.1. *Let* $f(x)$ *be a polynomial in* $\mathbb{Q}[x]$. *Then there exists a monic polynomial* $h(x) \in \mathbb{Z}[x]$ *such that* $\mathrm{Gal}(f) = \mathrm{Gal}(h)$.

Proof. Let $f(x) \in \mathbb{Q}[x]$; then $f(x) = \frac{1}{D}g(x)$, with $g(x) \in \mathbb{Z}[x]$ and D equal to a common denominator for the coefficients of f. Let $g(x) = \sum_{i=0}^{n} b_i x^i,\ b_i \in \mathbb{Z}$. Then

$$\begin{aligned} g(x) &= \frac{1}{b_n^{n-1}}\left((b_n x)^n + b_{n-1}(b_n x)^{n-1} + \cdots + b_1 b_n^{n-2}(b_n x) + b_0 b_n^{n-1}\right) \\ &= \frac{1}{b_n^{n-1}} h(b_n(x)), \end{aligned}$$

where $h(x) \in \mathbb{Z}[x]$ is monic. Hence

$$h(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1 b_n^{n-2} x + b_0 b_n^{n-1} = D b_n^{n-1} f\left(\frac{x}{b_n}\right).$$

It's easy to verify that $\mathrm{Gal}(f) = \mathrm{Gal}(h)$, since $\mathbb{Q}_f = \mathbb{Q}_h$. In fact, if $\alpha_1, \ldots, \alpha_n$ are n distinct roots of f, i.e. $\mathbb{Q}_f = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, then $\alpha_1 b_n, \ldots, \alpha_n b_n$ are n distinct roots of h, i.e. $\mathbb{Q}_h = \mathbb{Q}(\alpha_1 b_n, \ldots, \alpha_n b_n)$. But $b_n \in \mathbb{Z}$, so that

$$\mathbb{Q}_f = \mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(\alpha_1 b_n, \ldots, \alpha_n b_n) = \mathbb{Q}_h.$$

□

Thus we need consider only polynomials of the form

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n,\ a_i \in \mathbb{Z}.$$

Moreover we want $f(x)$ to be irreducible; this restiction is not essential, but it greatly simplifies the work of implementing the algorithm for polynomials of a given degree. By the way, let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial and $f(x) = g(x) \cdot h(x)$ be its decomposition into irreducible factors, $\mathbb{Q}_g$ and $\mathbb{Q}_h$ being the respective splitting fields. If $\mathbb{Q}_g \cap \mathbb{Q}_h = \mathbb{Q}$, then the Galois group of $f(x)$ is the direct product $\mathrm{Gal}(g) \times \mathrm{Gal}(h)$. Otherwise, if $\mathbb{Q}_g \cap \mathbb{Q}_h$ is larger than $\mathbb{Q}$, then $\mathrm{Gal}(f)$ is not easily determined from those of $g(x)$ and $h(x)$, without explicit knowledge of the relations between the roots of g and h. In fact, generally we have

$$\mathrm{Gal}(g \cdot h) = \{(\sigma_i, \sigma_j) \in \mathrm{Gal}(g) \times \mathrm{Gal}(h) \text{ s.t. } \sigma_i|_{\mathbb{Q}_g \cap \mathbb{Q}_h} = \sigma_j|_{\mathbb{Q}_g \cap \mathbb{Q}_h}\}.$$

With this assumptions, the strategy for determining the Galois group of a polynomial $f \in \mathbb{Z}[x]$ is:

1. test whether f is irreducible over $\mathbb{Z}$;
2. compute the discriminant $\Delta(f)$;
3. factor f modulo primes not dividing the discriminant until you seem to be getting no new decomposition type;
4. compute the orbit lengths on the r–sets of roots;
5. use tables of transitive groups of degree ∂f.

The second point is very useful. In fact, knowledge of $\Delta(f)$ allows us to establish if $\mathrm{Gal}(f) \subseteq A_n$.

Proposition 3.3.2. *Let A_n be the alternating group on n letters. Then $\mathrm{Gal}(f) \subset A_n$ if and only if $\Delta(f)$ is a square.*

Proof. Let α_i be the roots of f. We know that $D(f) = \Delta(f)^2$, where $\Delta(f) = \prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)$. Clearly $\Delta(f)$ is an algebraic integer, since it's a symmetric polynomial on $\alpha_1, \ldots, \alpha_n$. We have $\sigma(\Delta(f)) = \epsilon(\sigma)\Delta(f)\ \forall \sigma \in \mathrm{Gal}(f)$, where $\epsilon(\sigma)$ is the signature of σ. Hence, if $\mathrm{Gal}(f) \subset A_n$, then $\Delta(f)$ is invariant under $\mathrm{Gal}(f)$, and so $\Delta(f) \in \mathbb{Z}$. On the other hand, if $\Delta(f) \in \mathbb{Z}$, we have $\Delta(f) \neq 0$ since the root of an irreducible polynomial in $\mathbb{Z}[x]$ are distinct. Therefore $\sigma(\Delta(f)) = \Delta(f)$, that is $\epsilon(\sigma) = 1$, $\forall \sigma \in G$, and $\mathrm{Gal}(f) \subset A_n$. □

Remark 3.3.3. *Consider a permutation $\sigma \in S_n$,*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

and define $\eta(\sigma) = \{(i,j) \text{ with } i < j \text{ and } \sigma(i) > \sigma(j)\}$. Then σ is said to be even or odd according as the number $\eta(\sigma)$ is even or odd. The signature, $\epsilon(\sigma)$, of σ is $+1$ or -1 according as σ is even or odd, i.e., $\epsilon(\sigma) = (-1)^{\eta(\sigma)}$. With this definition of signature, it's easily seen that $\sigma(\Delta(f)) = \epsilon(\sigma)\Delta(f)$, as we stated above.

The third point is difficult to execute from a computational point of view: this is a rather expensive technique since algorithms of factorizing polynomials are not very efficient. Furthermore, many primes p might be needed in the process. For more detail on the problem, see [LO77].

The fourth point gives an upper bounds for $\mathrm{Gal}(f)$ using a method based on the following lemma. We refer to [EFM79] and [McK79].

Lemma 3.3.4. *Let $K_\alpha = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ and $K_\beta = \mathbb{Q}(\beta_1, \ldots, \beta_m)$, where $\{\beta_k\}$ is the set of the partial sums r at a time, with $0 < r < n$, of the $\{\alpha_i\}$ and $m = \#\{\beta_k\} = \binom{n}{r}$. Then $K_\alpha = K_\beta$.*

Proof. Let $r > 1$. For every i, j we have $\alpha_i - \alpha_j \in K_\beta$, since $\alpha_i - \alpha_j$ is the difference of two of the b's differing in one place. Suppose that $\beta_k = \sum_{j \in I} \alpha_j$, where $\#I = r$; then

$$\beta_k + \sum_{j \in I} (\alpha_i - \alpha_j) = r\alpha_i \in K_\beta.$$

□

If we denote with $P_\alpha = \prod(x - \alpha_i)$ and with $P_\beta = \prod(x - \beta_k)$, Lemma 3.3.4 yields $\mathrm{Gal}(P_\alpha) = \mathrm{Gal}(P_\beta)$. It's fundamental to notice that the degrees of the irreducible factors in $\mathbb{Q}[x]$ of the polynomial P_β, whose roots are the sums of r roots of P_α, equal the orbit lengths on the r–sets of roots. In particular the following holds.

Proposition 3.3.5. *Let P_β be the above polynomial and assume that it has only distinct zeros. Then P_β is reducible if and only if $\mathrm{Gal}(P_\alpha)$ is not r–transitive on $\{\alpha_i\}$.*

If we can prove by the Chebotarëv density theorem that

$$G \subseteq \mathrm{Gal}(f) \subseteq A_n,$$

where G is maximal in A_n, then Proposition 3.3.5 will usually determine $\mathrm{Gal}(f)$. In [McK79], the author describes and uses this method to find polynomials with Galois group $PSL_3(\mathbb{F}_2)$ and M_{11}: the first one is a maximal subgroup of the alternating group A_7, while the second one is the Mathieu group of degree 11, which is a maximal subgroup of A_{11}. Here below, we illustrate how this test works.

Example 3.3.6. *Let $P_\alpha(x) = x^5 - 5x + 12$ and A be the set of its roots, which we denote with $\{\alpha_1, \ldots, \alpha_5\}$. If $r = 2$, then $B = \{\alpha_1 + \alpha_2, \alpha_1 + \alpha_3, \alpha_1 + \alpha_4, \alpha_1 + \alpha_5, \alpha_2 + \alpha_3, \alpha_2 + \alpha_4, \alpha_2 + \alpha_5, \alpha_3 + \alpha_4, \alpha_3 + \alpha_5, \alpha_4 + \alpha_5\}$. Suppose, after several $\bmod p$ reductions, that we have two possibilities for $G = \mathrm{Gal}(P_\alpha)$, i.e. $D_5 \subseteq G \subseteq A_5$. Computing $P_\beta(x) = \prod_{\beta_i \in B}(x - \beta_i)$, we get*

$$P_\beta(x) = (x^5 - 5x^3 - 10x^2 - 30x - 36)(x^5 + 5x^3 + 10x^2 + 10x + 4).$$

Therefore $\mathrm{Gal}(P_\alpha)$ is not 2–transitive. This information gives us the desired upper bound: in fact, since A_n is $(n-2)$–transitive, the only possibility is $\mathrm{Gal}(P_\alpha) = D_5$.

Remark 3.3.7. *Proposition 3.3.5 gives information on r–fold transitivity, i.e. transitivity on r–sets, rather than on r–transitivity. However these two concepts are the same in many cases. In particular, for $r = 2$ we have that a group G is 2–transitive if and only if G is 2–fold transitive, and therefore the result in Example 3.3.6 is correct.*

Instead of making considerations on the r–fold transitivity, Soicher and McKay in [SM85] suggest to use the decomposition type of P_β in order to identify Gal(P_α), tabulating for each transitive group of degree up to 7 its specific decomposition on $\mathbb{Q}$ of P_β, that is the orbit length partition on r–sets under tha action of Gal(P_α). In Example 3.3.6, the decomposition type of P_β associated to D_5 is 5^2, while that one associated to A_5 is 10.
Although this strategy does not determine Gal(P_α) univocally, the information we can get in this way plays a fundamental role in distinguishing between group which appear very similar. In fact, the Chebotarëv test suggested at point 3 is not always effective: it gets into problems since it is possible to construct two non–isomorphic groups which have transitive permutation representations in which the number of elements with a given cycle structure is the same for both groups. This problem arises in degree 8 with polynomials

$$f(x) = x^8 - 3x^6 + 9x^4 - 12x^2 + 16 \text{ and } g(x) = x^8 - 18x^4 + 9.$$

According to Maple9, Gal$(f) = 8T_{10}$ and Gal$(g) = 8T_{11}$, but we can't get this result just by means of mod$p$ reduction. In fact $8T_{10}$ and $8T_{11}$ are not distinguishable if we just consider their cycle type distribution, as Table 3.3 shows. They are both groups of order 16 with generators

$$8T_{10} = \langle (1238)(4567), (15)(37) \rangle,$$

and

$$8T_{11} = \langle (15)(37), (2468)(1357), (1458)(2367) \rangle.$$

		2^2		
	1^8	1^4	2^4	4^2
$8T_{10}+$	1	2	5	8
$8T_{11}+$	1	2	5	8

Table 3.3: Cycle type distribution for $8T_{10}$ and $8T_{11}$.

In this situation, considerations on the orbit–length partition of r–sets are very useful. For example, if $r = 2$, the decomposition type of P_β relative to $8T_{10}$ is $(4^3, 16)$, while the one relative to $8T_{11}$ is $(8^3, 4)$. However, if $r = 2$, then P_β in Example 3.3.6 has multiple roots, and therefore we need a preliminar *Tschirnhausen transformation*, as explained in [SM85].

The informations, that we used, on the orbit–length partition of r–sets under the action of $G = Gal(f)$ can be found in [SM85] for transitive groups of degree up to 7 and in [MM97] for each transitive group of degree 8.

3.4 Transitive Groups

In this section we illustrate the tables for all transitive permutation groups of degrees 3 to 7 and 11, and include the distribution of cycle patterns and permutation generators. We will not analyze degree 8, 9, 10, 12, 13, 14, 15, etc. Below we tabulate the number of transitive subgroups of S_n, for n from 3 to 30, in order to give an idea of the complexity of some degrees; these informations are from [CHM98]. It's interesting to notice that when n is prime, the number of transitive groups is relatively low, but when it's not the case, the scenary is completely different. Numbers in italics are preliminary, and not yet confirmed.

Deg.	Transitive groups	Primitive groups	Deg.	Transitive groups	Primitive groups
2	1	1	17	10	10
3	2	2	18	983	4
4	5	2	19	8	8
5	5	5	20	1117	4
6	16	4	21	164	9
7	7	7	22	59	4
8	50	7	23	7	7
9	34	11	24	*26813*	5
10	45	9	25	211	28
11	8	8	26	96	7
12	301	6	27	*2382*	15
13	9	9	28	*1852*	14
14	63	4	29	8	8
15	104	6	30	*5712*	4
16	1954	22	31	12	12

Table 3.4: Number of transitive and primitivee groups of degree up to 31.

The following tables can be found in [BM83] for degree up to 11. The notation for the group names is similar to that one in [McK79]. For each degree we give a brief description of inclusions and geometric representation of groups. Groups marked $'+'$ are groups of even permutations.

Degree 3

The transitive subgroups of S_3 are $A_3 \simeq C_3 \simeq D_3$ and S_3.

Deg 3		2		
	1^3	1	3	$\#G$
A_3+	1	.	2	3
S_3	1	3	2	6

Table 3.5: Transitive groups of degree 3.

Degree 4

The transitive subgroups of S_4 are V_4 (the Klein Vierergruppe), C_4, D_4 (the dihedral group of degree 4, i.e., the symmetry group of a square), A_4 and S_4. Some inclusions are

$$A_4 \supset V_4 \text{ and } D_4 \supset C_4.$$

Deg 4		2		3		
	1^4	1^2	2^2	1	4	$\#G$
C_4	1	.	1	.	2	4
V_4+	1	.	3	.	.	4
D_4	1	2	3	.	2	8
A_4+	1	.	3	8	.	12
S_4	1	6	3	8	6	24

Table 3.6: Transitive groups of degree 4.

Degree 5

The transitive subgroups of S_5 are C_5, D_5 (the dihedral group of degree 5, i.e., the symmetries of a regular pentagon), F_{20} (the Frobenius group of order 20, i.e., the affine maps on $\mathbb{F}_5$), A_5 and S_5. The inclusions are

$$A_5 \supset D_5 \supset C_5 \text{ and } F_{20} \supset D_5,$$

meaning that C_5, D_5 and A_5 correspond to square discriminant, and F_{20} and S_5 to non–square discriminant. The groups C_5, D_5 and F_{20} are solvable groups, while A_5 is simple.

Deg 5		2	2^2	3	3	4		
	1^5	1^3	1	2	1^2	1	5	$\#G$
C_5+	1	.	.	.	.	.	4	5
D_5+	1	.	5	.	.	.	4	10
F_{20}	1	.	5	.	.	10	4	20
A_5+	1	.	15	.	20	.	24	60
S_5	1	10	15	20	20	30	24	120

Table 3.7: Transitive groups of degree 5.

Degree 6

We will not go into details about groups of degree 6, for the simple reason that there are quite a lot of them. For instance, S_3, S_4 and S_5 can all be considered as transitive subgroups of S_6. In fact, S_4 can be embedded transitively into S_6 in two fundamentally different ways, by $(123) \mapsto (123)(456)$, $(34) \mapsto (15)(36)$, and by $(123) \mapsto (123)(456)$, $(34) \mapsto (13)(24)(56)$. The second of these embeddings corresponds to S_4 as the rotation group of a cube, while the first is obtained by identifying S_4 with the full symmetry group of a tetrahedron and maps into A_6. The image of A_4 is the same under both maps, and is transitive in S_6 as well. The embedding of S_5 into S_6 can also be described geometrically, by considering S_5 as the full symmetry group of a dodecahedron, meaning that A_5 (the rotation group) is also transitive in S_6.

Deg 6						3						
		2	2^2		3	2		4	4	5		
	1^6	1^4	1^2	2^3	1^3	1	3^2	1^2	2	1	6	#G
C_6	1	.	.	1	.	.	2	.	.	.	2	6
S_3	1	.	.	3	.	.	2	.	.	.	.	6
D_6	1	.	3	4	.	.	2	.	.	.	2	12
A_4+	1	.	3	.	.	.	8	.	.	.	.	12
G_{18}	1	.	.	3	4	.	4	.	.	.	6	18
G_{24}	1	3	3	1	.	.	8	.	.	.	8	24
S_4+	1	.	9	.	.	.	8	.	6	.	.	24
S_4-	1	.	3	6	.	.	8	6	.	.	.	24
$G^1{}_{36}$	1	.	9	6	4	.	4	.	.	.	12	36
$G^2{}_{36}+$	1	.	9	.	4	.	4	.	18	.	.	36
G_{48}	1	3	9	7	.	.	8	6	6	.	8	48
$PSL_2(\mathbb{F}_5)+$	1	.	15	.	.	.	20	.	.	24	.	60
G_{72}	1	6	9	6	4	12	4	.	18	.	12	72
$PGL_2(\mathbb{F}_5)$	1	.	15	10	.	.	20	30	.	24	20	120
A_6+	1	.	45	.	40	.	40	.	90	144	.	360
S_6	1	15	45	15	40	120	40	90	90	144	120	720

Table 3.8: Transitive groups of degree 6.

Degree 7

The transitive subgroups of S_7 are C_7, D_7 (the dihedral group of degree 7, consisting of the symmetries of a regular heptagon), F_{21}, F_{42} (both Frobenius groups, consisting of affine transformations on $\mathbb{F}_7$), $PSL_2(\mathbb{F}_7)$ (the projective special linear group of 2×2 matrices over $\mathbb{F}_7$), A_7 and S_7. The groups C_7, D_7, F_{21} and F_{42} are solvable, while $PSL_2(\mathbb{F}_7)$ and A_7 are simple groups. The inclusions are

$$A_7 \supset PSL_2(\mathbb{F}_7) \supset F_{21} \supset C_7.$$

Moreover

$$F_{42} \supset F_{21} \text{ and } F_{42} \supset D_7 \supset C_7.$$

Deg 7						3		
		2	2^2	2^3	3	2	3	3^2
	1^7	1^5	1^3	1	1^4	1^2	2^2	1
C_7+	1	.	.	.	.	.	.	.
D_7	1	.	.	7	.	.	.	.
$F_{21}+$	1	.	.	.	.	.	.	14
F_{42}	1	.	.	7	.	.	.	14
$PSL_2(\mathbb{F}_7)+$	1	.	21	.	.	.	.	56
A_7+	1	.	105	.	70	.	210	280
S_7	1	21	105	105	70	420	210	280

Deg 7		4						
	4	2	4	5	5	6		
	1^3	1	3	1^2	2	1	7	$\#G$
C_7+	.	.	.	.	.	.	6	7
D_7	.	.	.	.	.	.	6	14
$F_{21}+$	.	.	.	.	.	.	6	21
F_{42}	.	.	.	.	.	14	6	42
$PSL_2(\mathbb{F}_7)+$	.	42	.	.	.	.	48	168
A_7+	.	630	.	504	.	.	720	2520
S_7	210	630	420	504	504	840	720	5040

Table 3.9: Transitive groups of degree 7.

Degree 11

The transitive subgroups of S_{11} are C_{11}, D_{11} (the dihedral group), F_{55}, F_{110} (both Frobenius groups), $PSL_2(\mathbb{F}_{11})$ (the projective special linear group), M_{11} (the Mathieu group), A_{11} and S_{11}. The inclusions are

$$A_{11} \supset M_{11} \supset PSL_2(\mathbb{F}_{11}) \supset F_{55} \supset C_{11}.$$

Then

$$F_{110} \supset F_{55} \text{ and } F_{110} \supset D_{11} \supset C_{11}.$$

Since there are 56 different partitions of 11, we don't give the cycle type of elements that belongs to A_n and S_n. However we remember that an element of cycle type 1^{a_1}, 2^{a_2}, $\ldots, k^{a_k}$ occurs $n!/\prod_{i=1}^{k} i^{a_i}(a_i!)$ in S_n.

Deg 11						
		2^4	2^5	3^3	4^2	
	$1^1 1$	1^3	1	1^2	1^3	$\#G$
$C_{11}+$	1	.	.	.	.	11
D_{11}	1	.	11	.	.	22
$F_{55}+$	1	.	.	.	.	55
F_{110}	1	.	11	.	.	110
$PSL_2(\mathbb{F}_{11})+$	1	55	.	110	.	660
$M_{11}+$	1	165	.	440	990	7920

Deg 11		6	8			
	5^2	3	2	10		
	1	2	1	1	11	$\#G$
$C_{11}+$	.	.	.	.	10	11
D_{11}	.	.	.	.	10	22
$F_{55}+$	44	.	.	.	10	55
F_{110}	44	.	.	44	10	110
$PSL_2(\mathbb{F}_{11})+$	264	110	.	.	120	660
$M_{11}+$	1584	1320	1980	.	1440	7920

Table 3.10: Transitive groups of degree 11.

Chapter 4

Inverse Galois Problem

4.1 Computing Galois Groups

Can any permutation group appear as the Galois group of a polynomial over the rationals? The answer is positive just for solvable groups and is due to Shafarevich, as explained in [Šaf54]. Shafarevich's argument, however, is not constructive and so does not produce a polynomial having a prescribed finite solvable group as a Galois group. For unsolvable groups, the question is an open problem. For example, let us consider the the Mathieu group M_{23}. It is a finite simlpe group of order $2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ and can be regarded as a transitive subgroup of S_{23}. However, it's not known if there exists a polynomial $f(x) \in \mathbb{Q}[x]$ such that $\mathrm{Gal}(f)$ is the M_{23}, as explained in [Völ96].

In the following tables, partially taken from [SM85], each transitive permutation group of degree from 3 to 7 and 11 is realised as a Galois group over the rationals. The proof of exactness of these results is verified by the galois( ) routine implemented in Maple9, which computes the exact Galois group of polynomials of degree up to 9. For polynomials of degree 11, we use the polgalois( ) routine implemented in GP/Pari, version 2.3.2, which can handle polynomial of degree up to 11.

G	$f(x)$	Remarks
A_3	x^3+x^2-2x-1	$\mathbb{Q}_f=\mathbb{Q}(\zeta_7+\zeta_7^{-1})$
S_3	x^3+2	
C_4	$x^4+x^3+x^2+x+1$	$\mathbb{Q}_f=\mathbb{Q}(\zeta_5)$
V_4	x^4+1	$\mathbb{Q}_f=\mathbb{Q}(\zeta_8)$
D_4	x^4+2	
A_4	$x^4+8x+12$	
S_4	x^4+x+1	
C_5	$x^5+x^4-4x^3-3x^2+3x+1$	$\mathbb{Q}_f=\mathbb{Q}(\zeta_{11}+\zeta_{11}^{-1})$
D_5	$x^5-5x+12$	
F_{20}	x^5+2	
A_5	$x^5+20x+16$	
S_5	x^5+x+3	
C_6	$x^6+x^5+x^4+x^3+x^2+x+1$	$\mathbb{Q}_f=\mathbb{Q}(\zeta_7)$
S_3	x^6+108	$\mathbb{Q}_f=\mathbb{Q}_{x^3+2}$
D_6	x^6+2	
A_4	x^6-3x^2-1	$\mathbb{Q}_f=\mathbb{Q}_{x^4+8x+12}$
G_{18}	x^6+3x^3+3	
G_{24}	x^6-3x^2+1	
S_4+	x^6-4x^2-1	$\mathbb{Q}_f=\mathbb{Q}_{x^4+x+1}$
S_4-	$x^6-3x^5+6x^4-7x^3+2x^2+x-4$	$\mathbb{Q}_f=\mathbb{Q}_{x^4+x+1}$
G_{36}^1	x^6+2x^3-2	
G_{36}^2	$x^6+6x^4+2x^3+9x^2+6x-4$	
G_{48}	x^6+2x^2+2	
$PSL_2(\mathbb{F}_5)$	x^6+6x^5-124	
G_{72}	$x^6+2x^4+2x^3+x^2+2x+2$	
$PGL_2(\mathbb{F}_5)$	$x^6+2x^5+3x^4+4x^3+5x^2+6x+7$	
A_6	x^6+6x^5+100	
S_6	x^6+x+1	

Table 4.1: (A) Polynomials $f(x)$ such that $\mathrm{Gal}(f)=G$.

G	$f(x)$	Remarks
C_7	$x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 +$ $+14x^2 - 9x + 1$	$\mathbb{Q}_f = \mathbb{Q}(\sum_{j=1}^{4} \zeta_{29}^{12j})$
D_7	$x^7 + 7x^3 + 7x^2 + 7x - 1$	
F_{21}	$x^7 - 14x^5 + 56x^3 - 56x + 22$	
F_{42}	$x^7 + 2$	
$PSL_2(\mathbb{F}_7)$	$x^7 - 7x + 3$	*Trinks'polynomial*
A_7	$x^7 - 56x - 48$	
S_7	$x^7 + x + 1$	
C_{11}	$x^{11} + x^{10} - 10x^9 - 9x^8 + 36x^7 + +28x^6 +$ $-56x^5 - 35x^4 + 35x^3 + 15x^2 - 6x - 1$	$\mathbb{Q}_f = \mathbb{Q}(\zeta_{23} + \zeta_{23}^{-1})$
D_{11}	$x^{11} - x^{10} + 5x^8 + 8x^5 + 6x^4 - x^3 + x^2 +$ $+3x + 1$	
F_{55}	$x^{11} - 33x^9 + 396x^7 - 2079x^5 +$ $+4455x^3 - 2673x - 243$	
F_{110}	$x^{11} + 2$	
$PSL_2(\mathbb{F}_{11})$	$x^{11} - 4x^{10} - 25x^9 + 81x^8 + 237x^7 +$ $-562x^6 - 1010x^5 + 1574x^4 + 1805x^3 +$ $-1586x^2 - 847x + 579$	
M_{11}	$x^{11} + 2x^{10} - 5x^9 + 50x^8 + 70x^7 - 232x^6 +$ $+796x^5 + 1400x^4 - 5075x^3 + 10950x^2 +$ $+2805x - 90$	
A_{11}	$x^{11} - x^9 + x^7 - x^6 + 2x^5 +$ $+x^4 - 2x^3 - x - 1$	
S_{11}	$x^{11} - x + 2$	

Table 4.2: (B) Polynomials $f(x)$ such that $\mathrm{Gal}(f) = G$.

In Appendix C we write down a Maple code which computes Galois groups of polynomials using the strategy suggested by the Chebotarëv theorem. We introduce the following definitions in order to describe the code step by step.

Definition 4.1.1. *Let n be a positive integer. We define $S(n)$ to be the ordered set of all the cycle type in the symmetric group S_n, where the order is the lexicographic one. The cardinality of this set equals the number of different partitions of n, which we will denote with $\pi(n)$.*

Example 4.1.2. *There are 5 different partitions of $n = 4$. Therefore the ordered set $S(4)$ equals*

$$\{(1^4);\ (1^2, 2);\ (2^2); (1^2, 3);\ (4)\}.$$

Definition 4.1.3. *Let G be a transitive group of degree n. We define the distribution–vector $S(G)$ to be the vector, with $\pi(n)$ components, whose j–th component represents the distribution, in G, of the j–cycle type of $S(n)$. Namely*

$$S(G)[i] := \frac{|\{\sigma \in G \textit{ s.t. } \sigma \textit{ has cycle type } S(n)[i]\}|}{|G|}.$$

Given an irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree n, we can construct a similar distribution–vector $S(f)$ in the following way. Fix a bound k and consider the primes $p \leq k$. For each prime not dividing $\Delta(f)$, store the decomposition type of $(f \bmod p)$. When each prime in the bound has been parsed, compute the frequency of each decomposition type. Now, each decomposition type can be regarded as a partition of n in which the numbers that make up the partition are the degrees of the irreducible factors of $(f \bmod p)$. Finally complete the empirical distribution–vector $S(f)$ with the frequency found in this way keeping the lexicographic order, so that

$$S(f)[i] := \frac{|\{p \leq k \text{ s.t. } p \nmid \Delta(f) \text{ and } (f \bmod p) \text{ has a cycle decomposition of the type S(n)[i]}\}|}{|\{p \leq k \text{ s.t. } p \nmid \Delta(f)\}|}.$$

Definition 4.1.4. *Let G be a transitive group of degree n and $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree n. We define the error–vector $E(G)$ to* *be the vector obtained as the difference $S(f) - S(G)$. Moreover, we denote with $\epsilon(G)$ the euclidean norm of $E(G)$.*

Now we are ready for describing our code.

Step 1. Input: an irreducible monic polynomial $f(x)$ and a bound k for the size of prime numbers considered.

Step 2. Select all primes $p \leq k$ such that $p \nmid \Delta(f)$ and, for each of these primes, compute the decomposition type of $(f \bmod p)$. In this way we will obtain an array of decompositions type.

Step 3. Looking at the precedent array, compute the frequency of each decomposition type in order to get the distribution–vector $S(f)$.

Step 4. For each transitive group G of degree ∂f, compute the error–vector $E(G)$.

Step 5. Evaluate the euclidean norm $\epsilon(G)$.

Step 6. Choose the transitive group G which gives place to the minimal value of $\epsilon(G)$.

Step 7. Output: the empirical distribution–vector relative to f, and the group G described above, which equals $\mathrm{Gal}(f)$ in virtue of the Chebotarëv theorem.

We implemented this method for polynomials of degree from 3 to 7, and 11. The following tables show the output produced by means of the Chebotarëv test, applied with the bound $p \leq 1000$, for degrees 3, 4, and 5.

Deg 3	2		
	1^3	1	3
A_3+	0.3333	.	0.6667
x^3+x^2-2x-1	0.3293	.	0.6707
S_3	0.1667	0.5	0.3333
x^3+2	0.1446	0.5181	0.3373

Table 4.3: Empirical and theoretical results for polynomials of degree 3.

Deg 4	2			3	
	1^4	1^2	2^2	1	4
C_4	0.25	.	0.25	.	0.5
$x^4+x^3+x^2+x+1$	0.2395	.	0.2275	.	0.5329
V_4+	0.25	.	0.75	.	.
x^4+1	0.2216	.	0.7784	.	.
D_4	0.125	0.25	0.375	.	0.25
x^4+2	0.0838	0.2635	0.3952	.	0.2575
A_4+	0.0833	.	0.25	0.6667	.
$x^4+8x+12$	0.0723	.	0.2651	0.6627	.
S_4	0.0417	0.25	0.125	0.333	0.25
x^4+x+1	0.0179	0.2575	0.1257	0.3593	0.2395

Table 4.4: Empirical and theoretical results for polynomials of degree 4.

Deg 5		2	2^2	3	3	4	
	1^5	1^3	1	2	1^2	1	5
C_5+	0.2	.	.	.	.	.	0.8
$x^5 + x^4 - 4x^3 +$	0.1976	.	.	.	.	.	0.8024
$-3x^2 + 3x + 1$							
D_5+	0.1	.	0.5	.	.	.	0.4
$x^5 - 5x + 12$	0.0663	.	0.5120	.	.	.	0.4217
F_{20}	0.05	.	0.25	.	.	0.5	0.2
$x^5 + 2$	0.0482	.	0.2289	.	.	0.5301	0.1928
A_5+	0.0167	.	0.25	.	0.3333	.	0.4
$x^5 + 20x + 16$	0.0060	.	0.2711	.	0.3133	.	0.4096
S_5	0.0083	0.0833	0.125	0.1667	0.1667	0.25	0.2
$x^5 + x + 3$	0	0.0952	0.1488	0.1786	0.1426	0.2262	0.2083

Table 4.5: Empirical and theoretical results for polynomials of degree 5.

In the following tables we compare, with respect to $\epsilon(G)$, the error–vectors $E(G)$ defined in 4.1.4, for polynomials of the type

$$f(x) = x^n + 2,$$

where $n \in \{3, 4, 5, 6, 7, 11\}$. The minimal value of ϵ is always obtained for the transitive group G of degree n and order $|G| = n \cdot \varphi(n)$, as Galois theory predicts. The bound considered is $p \leq 1000$, which is always effective in these examples.

$\epsilon(S_3)$	$\epsilon(A_3)$
0.0288	0.6422

Table 4.6: Computation of $\epsilon(G)$ for $x^3 + 2$.

$\epsilon(S_4)$	$\epsilon(A_4)$	$\epsilon(C_4)$	$\epsilon(D_4)$	$\epsilon(V_4)$
0.4314	0.7754	0.4206	0.0484	0.5378

Table 4.7: Computation of $\epsilon(G)$ for $x^4 + 2$.

$\epsilon(S_5)$	$\epsilon(A_5)$	$\epsilon(F_{20})$	$\epsilon(D_5)$	$\epsilon(C_5)$
0.3917	0.6607	0.0375	0.6326	0.8516

Table 4.8: Computation of $\epsilon(G)$ for $x^5 + 2$.

$\epsilon(S_6)$	$\epsilon(A_6)$	$\epsilon(PGL_2(\mathbb{F}_5))$	$\epsilon(G_{42})$
0.5059	0.6367	0.4343	0.4427
$\epsilon(PSL_2(\mathbb{F}_5))$	$\epsilon(G_{48})$	$\epsilon(G_{36}^2)$	$\epsilon(G_{36}^1)$
0.5833	0.2816	0.6422	0.2615
$\epsilon(S_4-)$	$\epsilon(S_4+)$	$\epsilon(G_{24})$	$\epsilon(G_{18})$
0.3906	0.5042	0.4197	0.4163
$\epsilon(A_4)$	$\epsilon(D_6)$	$\epsilon(S_3)$	$\epsilon(C_6)$
0.6379	0.0262	0.4093	0.4010

Table 4.9: Computation of $\epsilon(G)$ for $x^6 + 2$.

$\epsilon(S_7)$	$\epsilon(A_7)$	$\epsilon(PSL_2(\mathbb{F}_7))$	$\epsilon(F_{42})$	$\epsilon(F_{21})$	$\epsilon(D_7)$	$\epsilon(C_7)$
0.4197	0.5694	0.4997	0.03163	0.5448	0.6469	0.8750

Table 4.10: Computation of $\epsilon(G)$ for $x^7 + 2$.

$\epsilon(S_{11})$	$\epsilon(A_{11})$	$\epsilon(M_{11})$	$\epsilon(PSL_2(\mathbb{F}_{11}))$	$\epsilon(F_{110})$	$\epsilon(F_{55})$	$\epsilon(D_{11})$	$\epsilon(C_{11})$
0.5202	0.6028	0.5727	0.4919	0.0084	0.5844	0.7834	0.9989

Table 4.11: Computation of $\epsilon(G)$ for $x^{11} + 2$.

Finally, in the tables below we give an idea of the accuracy of our results, which depends on the choice of the upper bound k representing the size of prime numbers that we want to consider. If we increase k, on the one hand our result will be more precise, on the other hand Maple will need more time to produce the output.
The polynomials considered are those in Table 4.1 and 4.2 with Galois group A_n, as we can guess comparing the norm $\epsilon(A_n)$ with $\epsilon(G)$, for each other transitive group G of degree n.

k	Time	$\epsilon(S_3)$	$\epsilon(A_3)$
10^2	0.01s	0.6374	0.0589
10^3	0.3s	0.6247	0.0056
10^4	2.1s	0.6250	0.0073
10^5	22.4s	0.6238	0.0012
10^6	696.9s	0.6237	0.0002

Table 4.12: Comparing $\epsilon(G)$ with respect to k. Degree 3

k	Time	$\epsilon(S_4)$	$\epsilon(A_4)$	$\epsilon(C_4)$	$\epsilon(D_4)$	$\epsilon(V_4)$
10^2	0.01s	0.5242	0.0504	0.8813	0.7928	0.8751
10^3	0.3s	0.5039	0.0191	0.8491	0.7609	0.8402
10^4	2.3s	0.5056	0.0051	0.8536	0.7699	0.8544
10^5	25.1s	0.5039	0.0018	0.8506	0.7665	0.8501
10^6	765.1s	0.5035	0.0003	0.8499	0.7660	0.8497

Table 4.13: Comparing $\epsilon(G)$ with respect to k. Degree 4

k	Time	$\epsilon(S_5)$	$\epsilon(A_5)$	$\epsilon(F_{20})$	$\epsilon(D_5)$	$\epsilon(C_5)$
10^2	0.01s	0.4582	0.1114	0.6758	0.4934	0.5429
10^3	0.3s	0.4289	0.0325	0.6281	0.3993	0.6014
10^4	2.2s	0.4254	0.0321	0.6396	0.4413	0.6360
10^5	24.8s	0.4255	0.0023	0.6341	0.4239	0.6044
10^6	700.3s	0.4252	0.0008	0.6343	0.4248	0.6054

Table 4.14: Comparing $\epsilon(G)$ with respect to k. Degree 5

k	Time	$\epsilon(S_6)$	$\epsilon(A_6)$	$\epsilon(PGL_2(\mathbb{F}_5))$	$\epsilon(G_{72})$	$\epsilon(PSL_2(\mathbb{F}_5))$	$\epsilon(G_{48})$	$\epsilon(G_{36}^2)$	$\epsilon(G_{36}^1)$
10^2	0.01s	0.4977	0.2516	0.6212	0.5791	0.5699	0.6513	0.5304	0.7738
10^3	0.3s	0.3906	0.0696	0.4796	0.5184	0.3808	0.5449	0.5291	0.6519
10^4	2.9s	0.3691	0.0189	0.4647	0.4787	0.3807	0.5095	0.4785	0.6131
10^5	30.8s	0.3725	0.0038	0.4654	0.4879	0.3754	0.5164	0.4914	0.6171
10^6	948.4s	0.3710	0.0016	0.4641	0.4848	0.3750	0.5133	0.4874	0.6145

Table 4.15: (A) Comparing $\epsilon(G)$ with respect to k. Degree 6.

k	Time	$\epsilon(S_4-)$	$\epsilon(S_4+)$	$\epsilon(G_{24})$	$\epsilon(G_{18})$
10^2	0.01s	0.8057	0.6706	0.8079	0.8126
10^3	0.3s	0.6552	0.5719	0.6578	0.6501
10^4	2.9s	0.6364	0.5296	0.6391	0.6287
10^5	30.8s	0.6433	0.5379	0.6459	0.6382
10^6	948.4s	0.6407	0.5340	0.6434	0.6358

k	Time	$\epsilon(A_4)$	$\epsilon(D_6)$	$\epsilon(S_3)$	$\epsilon(C_6)$
10^2	0.01s	0.9412	0.7797	0.8991	0.8350
10^3	0.3s	0.7602	0.6636	0.7635	0.6869
10^4	2.9s	0.7466	0.6309	0.7544	0.6768
10^5	30.8s	0.7548	0.6341	0.7613	0.6844
10^6	948.4s	0.7519	0.6316	0.7591	0.6821

Table 4.16: (B) Comparing $\epsilon(G)$ with respect to k. Degree 6

k	Time	$\epsilon(S_7)$	$\epsilon(A_7)$	$\epsilon(PSL_2(\mathbb{F}_7))$
10^2	0.01s	0.3459	0.1069	0.3172
10^3	0.3s	0.3280	0.0346	0.3475
10^4	3.4s	0.3267	0.0131	0.3200
10^5	33.5s	0.3269	0.0113	0.3234
10^6	950.2s	0.3248	0.0036	0.3255

Table 4.17: (A) Comparing $\epsilon(G)$ with respect to k. Degree 7.

k	Time	$\epsilon(F_{42})$	$\epsilon(F_{21})$	$\epsilon(D_7)$	$\epsilon(C_7)$
10^2	0.01s	0.5741	0.6499	0.5918	0.5957
10^3	0.3s	0.5776	0.6666	0.6436	0.7049
10^4	3.4s	0.5675	0.6496	0.6273	0.6753
10^5	33.5s	0.5672	0.6488	0.6288	0.6778
10^6	950.2s	0.5679	0.6519	0.6318	0.6853

Table 4.18: (B) Comparing $\epsilon(G)$ with respect to k. Degree 7.

k	Time	$\epsilon(S_{11})$	$\epsilon(A_{11})$	$\epsilon(M_{11})$	$\epsilon(PSL_2(\mathbb{F}_{11}))$
10^2	0.3s	0.3428	0.2399	0.4033	0.4465
10^3	1.3s	0.2309	0.0769	0.3269	0.4521
10^4	9.2s	0.2149	0.0278	0.3232	0.4767
10^5	94.1s	0.2133	0.0093	0.3257	0.4775
10^6	1878s	0.2128	0.0034	0.3268	0.4770
k	Time	$\epsilon(F_{110})$	$\epsilon(F_{55})$	$\epsilon(D_{11})$	$\epsilon(C_{11})$
10^2	0.3s	0.6208	0.7680	0.5892	0.6587
10^3	1.3s	0.5959	0.7784	0.6183	0.7622
10^4	9.2s	0.6075	0.8018	0.6206	0.7718
10^5	94.1s	0.6037	0.7965	0.6190	0.7698
10^6	1878s	0.6036	0.7966	0.6204	0.7722

Table 4.19: Comparing $\epsilon(G)$ with respect to k.

The norm $\epsilon(G)$ can be regarded as a measure of the distance between the theoretical and the empirical result.

Definition 4.1.5. *We call $\epsilon(G)$ the relative error of G.*

It's clear that $\epsilon(G) = \epsilon(G, k)$. From the analysis of the relative errors we notice that

$$\epsilon(A_n,\, 10^6) < 10^{-2} \text{ and } \epsilon(A_n,\, 10^3) < 10^{-1},$$

and, by induction, one may naively guess $\epsilon(G,\, 10^{3t}) < 10^{-t}$, $t \geq 1$, where G equals $\mathrm{Gal}(f)$. This observation shows that $k \geq 10^3$ usually is a good bound for the Chebotarëv test.

4.2 Groups of Prime Degree Polynomials

Computing Galois groups is still a difficult task. Even with the development of new computer algebra systems this remains a challenge and can be accomplished only for small degree polynomials. For example, Maple9 can only handle polynomials of degree ≤ 9 and GP/Pari up to degree 11. Other computer algebra packages can handle polynomials whose degree is in the same range. The existence of non–real roots of a polynomial makes the computation of its Galois group much easier. Computing the Galois group in this case, for polynomials of prime degree p, will be the focus of this section. Checking whether a polynomial has non–real roots is very efficient since numerical methods can be used. Once the existence of non–real roots is established then from a theorem of Jordan (1871) it follows that if their number is small enough with respect to the degree p of the polynomial, then the Galois group is A_p or S_p. Furthermore, knowledge of the complete classification of transitive groups of prime degree enables us to provide a complete list of possible Galois groups for every irreducible polynomial of prime degree p which has non–real roots.

By degree of a permutation group $G \subseteq S_n$ we mean the number of points in $\{1, \dots, n\}$ moved by G. The degree of a permutation $\alpha \in S_n$ is the number of points moved by $\langle\alpha\rangle$. The minimal degree of G, denoted by $m(G)$, is the smallest of degrees of elements $\alpha \neq 1$ in G. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree $n \geq 5$. Denote by r the number of non-real roots of $f(x)$. Since the complex conjugation permutes the roots then r is even, say $r = 2s$, by a reordering of the roots and we may assume that if $f(x)$ has r non–real roots then

$$\alpha := (1,2)(3,4)\cdots(r-1,r) \in \mathrm{Gal}(f)$$

is the complex conjugation Since determining the number of non–real roots can be very fast, we would like to know to what extent the number of non–real roots of $f(x)$ determines $\mathrm{Gal}(f)$. The complex conjugation assures that $m(G) \leq r$. The existence of α can narrow down the list of candidates for $\mathrm{Gal}(f)$.

Example 4.2.1. *Let $f(x) = 48x^7 - 56x^6 + 7$ be an irreducible polynomial. From a simple computation we discover that the number of real roots of $f(x)$ is 3, and so there exists an elemente $\alpha \in \mathrm{Gal}(f)$ of the form $(1,2)(3,4)$, which permutes 4 complex roots of $f(x)$.*
Looking at the Table 3.9 of transitive group of order 7, we find that possible candidates for $\mathrm{Gal}(f)$ are S_7, A_7, $PSL_2(\mathbb{F}_7)$. Then one can use other tools, like computation of $\Delta(f)$ and $\bmod\, p$ reductions, to determine this group univocally.

In despite of the example above, it is unlikely that the group can be determined only from this information unless p is "large" enough. In this case the number of non–real roots of $f(x)$ can almost determine the Galois group of $f(x)$, as we will see. Nevertheless, the test is worth running for all p since it is very fast and improves the algorithm overall.
Next theorem determines the Galois group of a prime degree polynomial $f(x)$ with r non–real roots when the degree of $f(x)$ is large enough with respect to r. We refer to [Ser03] for a more extensive description of the following results.

Theorem 4.2.2. *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree $p \geq 3$ and $r = 2s$ be the number of non–real roots of $f(x)$. If s satisfies*

$$s(slogs + 2logs + 3) \leq p$$

then $\mathrm{Gal}(f) = A_p$, *or* S_p.

Proof. Since p is prime, every transitive subgroup of S_p is primitive (see [Rot95]). Let G denote the Galois group of $f(x)$ and $m(G)$ its minimal degree. By reordering the roots we can assume that

$$(1, 2)(3, 4) \cdots (r - 1, r) \in \mathrm{Gal}(f).$$

Hence, $m := m(G) \leq r$. From the theorem of Jordan discussed in [Jor72] we have that

$$\frac{m^2}{4} \log \frac{m}{2} + m \left(\log \frac{m}{2} + \frac{3}{2} \right) \leq p \Rightarrow G = A_p \text{ or } S_p.$$

Hence, if we consider $r = 2s$ instead of m, we have that if

$$s(slogs + 2logs + 3) \leq p$$

then $G = A_p$ or S_p. □

For a fixed p the above bound is not sharp as we will see below. However, Theorem 4.2.2 can be used successfully if s is fixed. We denote the above lower bound on p by $N(r) := [s(slogs + 2logs + 3)]$ for $r = 2s$. Hence, for a fixed number of non–real roots and for $p \geq N(r)$ the Galois group is always A_p or S_p.

Corollary 4.2.3. *Let a polynomial of prime degree p and assume that r denotes the number of its non-real roots. If one of the following holds:*

(i) $r = 2$ *and* $p > 2$,

(ii) $r = 4$ *and* $p > 7$,

(iii) $r = 6$ *and* $p > 13$,

(iv) $r = 8$ *and* $p > 23$*,*

(v) $r = 10$ *and* $p > 37$*,*

then $\mathrm{Gal}(f) = A_p$ *or* S_p*.*

Remark 4.2.4. *The above results gives a very quick way of determining the Galois group for polynomials with non–real roots. Whether or not the discriminant is a complete square can be used to distinguish between* A_p *and* S_p*. In the case* (i), (iii), (v)*, it's very easy to choose between* A_p *and* S_p*; in fact we have obviously that* $\mathrm{Gal}(f) = S_p$*, since the complex conjugation is an odd permutation.*

If $p < N(r)$ then some exceptional cases occur. We remark that if we consider $f(x)$ such that $\partial f = p \leq 29$, no two groups have the same cycle structure, and so the Galois group can be determined uniquely by reduction modulo p for all polynomials of prime degree ≤ 29 with non–real roots.

Example 4.2.5. *Let* $f(x) = x^7 - 4x^6 - 20x^5 + 4x^4 + 20x^3 + 2$*. This polynomial is irreducible over* $\mathbb{Q}$ *and has exactly* 2 *non–real roots. We can easily check these facts in Maple9 using the commands*

```
f:=x^7-4*x^6-20*x^5+4*x^4+20*x^3+2;
factor(f);
realroot(f);
```

From Corollary 4.2.3, $\mathrm{Gal}(f)$ *is* S_7 *or* A_7*. Its discriminant is* $\Delta(f) = -(2)^6 \cdot (3)^3 \cdot (47031541) \cdot (4289)$*, which is* ≤ 0*; therefore it is not a square in* $\mathbb{Q}$ *and the Galois group of* $f(x)$ *is* S_7*, as we can verify with the command*

```
galois(x^7-4*x^6-20*x^5+4*x^4+20*x^3+2);
"7T7", {"S(7)"}, "-", 5040;
```

Combining the above results we have the following algorithm for computing the Galois group of prime degree polynomials with non–real roots. Note that even in the case $p < N(r)$ we know that a permutation of the type $(2)^{\frac{r}{2}}$

is in the group. Hence, the list of transitive subgroups is much shorter than in general. This information was obtained by computing the number of real roots rather then by some factorization modulo p. Thus, even in this case the algorithm can be improved.

Algorithm: Computing the Galois group of prime degree polynomials with few non–real roots.

Input: an irreducible monic polynomial $f(x) \in \mathbb{Z}[x]$ of prime degree p.

Output: Galois group of $f(x)$ over $\mathbb{Q}$.

```
begin
r:=Number Of Real Roots(f(x));
  if p > N(r) {
    if D(f) is a square {
      Gal(f)=A_p;
    else Gal(f) = S_p;
    }
  else Chebotarev test(f(x));
  }
end;
```

Example 4.2.6. *Let* $f(x) = x^{11}+4x^{10}-14x^9-56x^8+50x^7+200x^6-50x^5-200x^4+49x^3+196x^2-36x-143$ *be irreducible over* $\mathbb{Q}$. *We get*

```
nops(realroot(f));
7
```

In fact $f(x)$ *has been produced expanding* $(x^4+1)(x+4)\prod_{j=1}^{3}(x\pm j)+1$, *which is proved to be irreducible. In this case* $r = 11 - 7 = 4$ *and* $N(r) \approx 8.41$, *which is* $\leq p = 11$. *We are in the conditions of Corollary 4.2.3, hence* $\mathrm{Gal}(f) = S_{11}$ *or* A_{11}. *Computing discriminant we observe that it's not a square and therefore*

$$\mathrm{Gal}(f) \nsubseteq A_{11} \Rightarrow \mathrm{Gal}(f) = S_{11}.$$

Appendix A

Roots on Finite Fields

In this appendix we study the form of the roots of an irreducible polynomial in a finite fields of characteristic q. The following results are from [LN94].

Theorem A.0.7. *Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m; then $f(x)$ has a root in $\mathbb{F}_{q^m}$. Moreover, if $f(\alpha) = 0$, all the m distinct roots of f have molteplicity* 1 *and they are of the form*

$$\alpha^{q^h} \in \mathbb{F}_{q^m}, \text{ for all } 0 \leq h \leq m-1.$$

Proof. Let α be such that $f(\alpha) = 0$; then $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, i.e. $\mathbb{F}_q(\alpha) \simeq \mathbb{F}_{q^m}$ and we can consider α as an element in $\mathbb{F}_{q^m}$. We will show that $f(\beta) = 0$ implies (β^q), for any $\beta \in \mathbb{F}_{q^m}$. Let $f(x) = \sum_{i=0}^m a_i x^i, \ a_i \in \mathbb{F}_q$; then

$$\begin{aligned}
f(\beta^q) &= a_m\beta^{qm} + a_{m-1}\beta^{q(m-1)} + \cdots + a_1\beta^q + a_0 \\
&= a_m^q\beta^{qm} + a_{m-1}^q\beta^{q(m-1)} + \cdots + a_1^q\beta^q + a_0^q \\
&= (a_m\beta^m + a_{m-1}\beta^{m-1} + \cdots + a_1\beta + a_0)^q \\
&= [f(\beta)]^q \\
&= 0.
\end{aligned}$$

From this observation we conclude that if α is a root, then α^p, α^{p^2}, ..., $\alpha^{q^{m-1}}$ are roots of f. We will show that these roots are distinct. If there exist j, k such that $\alpha^{q^j} = \alpha^{q^k}$, with $0 \leq j < k \leq m-1$, then $\alpha^{q^{j+m-k}} = \alpha^{q^m}$ and therefore $\alpha^{q^{j+m-k}} = \alpha$, that is, α is a root of $x^{q^{j+m-k}} - x$. Hence $f(x)$ must di divide $x^{q^{j+m-k}} - x$, but from Lemma A.0.8 $f | x^{q^{j+m-k}} - x \Leftrightarrow \partial f = m | m - j + k$. Now, $0 < m - k + j < m$, and if $m | m - k + j$ we have an absurd. □

Lemma A.0.8. *Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m; then $f(x) | x^{q^n} - x \Leftrightarrow \partial f = m | n$.*

Proof. ($\Rightarrow$) We assume that $f(x) | x^{q^n} - x$; let α be a root of $f(x)$; then $\alpha^{q^n} = \alpha \Leftrightarrow \alpha \in \mathbb{F}_{q^n} \Leftrightarrow \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^n}$. But $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ and $[\mathbb{F}_q^n : \mathbb{F}_q] = n$ imply that $n = [\mathbb{F}_q^n : \mathbb{F}_q(\alpha)] \cdot m$, and so $m | n$.
($\Leftarrow$) It is easily seen that $m | n \Leftrightarrow \mathbb{F}_{q^n} \supset \mathbb{F}_{q^m}$. If α is a root of $f(x)$, then $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, and therefore $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$. So $\alpha \in \mathbb{F}_{q^n}$ or, in other words, $\alpha^{q^n} = \alpha$, that is, α is a root of $x^{q^n} - x \in \mathbb{F}_q[x]$. In short, $f(x) | x^{q^n} - x$. □

Appendix B

Galois Groups on Finite Fields

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field of p elements. Any other field E of characteristic p contains a copy of $\mathbb{F}_p$, namely, $\{m1_E : m \in \mathbb{Z}\}$. No harm results if we identify $\mathbb{F}_p$ with this subfield of E. Let E be a field of degree n over $\mathbb{F}_p$. Then E has $q = p^n$ elements, and so $E^* = E - \{0\}$ is a group of order $q-1$. Hence the nonzero elements of E are roots $x^{q-1} - 1$, and all elements of E, including 0, are roots of $x^q - x$. Hence E is a splitting field for $x^q - x$, and so any two fields with q elements are isomorphic.

Now let E be the splitting field of $f(x) = x^q - x$, $q = p^n$. The formal derivative $f'(x) \equiv -1 \bmod p$ is relatively prime to $f(x)$ and so $f(x)$ has q distinct roots in E. Let S be the set of its roots. Then S is obviously closed under multiplication and the formation of inverses, but it is also closed under subtraction; if $a^q = a$ and $b^q = b$, then

$$(a-b)^q = a^q - b^q = a - b.$$

Hence S is a field, and so $S = E$. In particular, E has p^n elements.

Proposition B.0.9. *For each power $q = p^n$ there is a field $\mathbb{F}_q$ with q elements. It is the splitting field of $x^q - x$, and hence any two such fields are isomorphic. Moreover, $\mathbb{F}_q$ is Galois over $\mathbb{F}_p$ with cyclic Galois group generated by the Frobenius automorphism $\sigma : a \mapsto a^p$.*

Proof. The field $\mathbb{F}_q$ is Galois over F_p because it is the splitting field of a separable polynomial $f(x)$, namely $x^q - x$. We noted that $\sigma : x \mapsto x^p$ is an automorphism of $\mathbb{F}_q$, sending each root $f(x)$ into another one, for Theorem A.0.7. An element $a \in \mathbb{F}_q$ is fixed by σ if and only if $a^p = a$; but $\mathbb{F}_p$ consists exactly of such elements, and so the fixed field of $\langle\sigma\rangle$ is $\mathbb{F}_p$. This proves that $\mathbb{F}_q$ is Galois over $\mathbb{F}_p$ and that $\langle\sigma\rangle = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. □

Appendix C

The Chebotarëv Test in Maple

Here we implement the modulo p reductions test suggested by Chebotarëv's theorem. The reader can run this program just by copying the code below in a Maple Worksheet and writing

```
Chebotarev(f(x),k);
```

where $f(x)$ is an irreducible polynomial of degree $n \in \{3, 4, 5, 6, 7, 11\}$ and k is the upper bound for the size of prime numbers that we want to consider. If we increase k, on the one hand our result will be more precise, on the other hand Maple will need more time to produce the output.
This tool allows us to make several experiments in finding polynomial with a given Galois group. In our attempts, we ran this program for all the polynomials in Table 4.1 and 4.2, with $k = 1000$, obtaining always the correct output, as shown in Section 4.1.

```
with(linalg);


Chebotarev3:=proc(list,nu)
local i,dt3,dt2,dt1,perc;
dt3:=0;dt2:=0;dt1:=0;
for i from 1 to nu do
if member(3,list[i]) then dt3:=dt3+1 else
if verify(list[i],[0,1,2],sublist) then dt2:=dt2+1 else
if verify(list[i],[0,1,1,1],sublist) then dt1:=dt1+1 fi;
fi;fi;
od;
print((0,0,3)=dt3/nu);
print((0,1,2)=dt2/nu);
print((1,1,1)=dt1/nu);
perc:=array(1..nu,[dt1/nu,dt2/nu,dt3/nu]);
getGroup3(perc);
end:

getGroup3:=proc(a)
local i,b,c;
c:=array(1..3,[1/3,0  ,2/3]);
b:=array(1..3,[1/6,1/2,1/3]);
for i from 1 to 3 do
b[i]:=a[i]-b[i];c[i]:=a[i]-c[i];
od;
if evalf(norm(c,frobenius))<evalf(norm(b,frobenius)) then
print("Gruppo A(3)") else print("Gruppo S(3)") fi;
end:


Chebotarev4:=proc(list,nu)
local i,dt5,dt4,dt3,dt2,dt1,perc;
dt5:=0;dt4:=0;dt3:=0;dt2:=0;dt1:=0;
for i from 1 to nu do
if member(4,list[i]) then dt5:=dt5+1 else
if verify(list[i],[0,1,3],sublist) then dt4:=dt4+1 else
if verify(list[i],[0,2,2],sublist) then dt3:=dt3+1 else
if verify(list[i],[0,1,1,2],sublist) then dt2:=dt2+1 else
if verify(list[i],[0,1,1,1,1],sublist) then dt1:=dt1+1 fi;
fi;fi;fi;fi;
od;
print((0,0,0,4)=dt5/nu);
print((0,0,1,3)=dt4/nu);
print((0,0,2,2)=dt3/nu);
print((0,1,1,2)=dt2/nu);
print((1,1,1,1)=dt1/nu);
perc:=array(1..nu,[dt1/nu,dt2/nu,dt3/nu,dt4/nu,dt5/nu]);
getGroup4(perc);
end:

getGroup4:=proc(a)
local i,s,b,c,d,e,f;
b:=array(1..5,[1/24,1/4,1/8,1/3,1/4]);
c:=array(1..5,[1/12,0  ,1/4,2/3,0  ]);
d:=array(1..5,[1/4 ,0  ,1/4,0  ,1/2]);
e:=array(1..5,[1/8 ,1/4,3/8,0  ,1/4]);
f:=array(1..5,[1/4 ,0  ,3/4,0  ,0  ]);
c:=array(1..5,[1/12,0  ,1/4,2/3,0  ]);
for i from 1 to 5 do
b[i]:=a[i]-b[i];c[i]:=a[i]-c[i]; d[i]:=a[i]-d[i];
e[i]:=a[i]-e[i];f[i]:=a[i]-f[i];
od;
s:=sort([evalf(norm(b,frobenius)),evalf(norm(c,frobenius)),
evalf(norm(d,frobenius)),evalf(norm(e,frobenius)),
evalf(norm(f,frobenius))]);
if s[1]= evalf(norm(b,frobenius))
then print("Gruppo S(4)") fi;
if s[1]= evalf(norm(c,frobenius))
then print("Gruppo A(4)") fi;
```

```
if s[1]= evalf(norm(d,frobenius))
then print("Gruppo C(4)") fi;
if s[1]= evalf(norm(e,frobenius))
then print("Gruppo D(4)") fi;
if s[1]= evalf(norm(f,frobenius))
then print("Gruppo C(2)xC(2)") fi;
end:

Chebotarev5:=proc(list,nu)
local i,dt7,dt6,dt5,dt4,dt3,dt2,dt1,perc;
dt7:=0;dt6:=0;dt5:=0;dt4:=0;dt3:=0;dt2:=0;dt1:=0;
for i from 1 to nu do
if member(5,list[i]) then dt7:=dt7+1 else
if verify(list[i],[0,1,4],sublist) then dt6:=dt6+1 else
if verify(list[i],[0,1,1,3],sublist) then dt5:=dt5+1 else
if verify(list[i],[0,2,3],sublist) then dt4:=dt4+1 else
if verify(list[i],[0,1,2,2],sublist) then dt3:=dt3+1 else
if verify(list[i],[0,1,1,1,2],sublist)
then dt2:=dt2+1 else
if verify(list[i],[0,1,1,1,1,1],sublist)
then dt1:=dt1+1 fi;fi;
fi;fi;fi;fi;fi;
od;
print((0,0,0,0,5)=dt7/nu);
print((0,0,0,1,4)=dt6/nu);
print((0,0,0,2,3)=dt5/nu);
print((0,0,1,1,3)=dt4/nu);
print((0,0,1,2,2)=dt3/nu);
print((0,1,1,1,2)=dt2/nu);
print((1,1,1,1,1)=dt1/nu);
perc:=array(1..nu,[dt1/nu,dt2/nu,dt3/nu,
dt4/nu,dt5/nu,dt6/nu,dt7/nu]);
getGroup5(perc);
end:

getGroup5:=proc(a)
local i,s,b,c,d,e,f,g,h;
b:=array(1..7,[1/120,1/12,1/8,1/6,1/6,1/4,1/5]);
c:=array(1..7,[1/60 ,0   ,1/4,0  ,1/3,0  ,2/5]);
d:=array(1..7,[1/20,0  ,1/4,0 ,0 ,1/2,1/5]);
e:=array(1..7,[1/10,0  ,1/2,0 ,0 ,0  ,2/5]);
f:=array(1..7,[1/5 ,0  ,0  ,0 ,0 ,0  ,4/5]);
for i from 1 to 7 do
b[i]:=a[i]-b[i];c[i]:=a[i]-c[i]; d[i]:=a[i]-d[i];
e[i]:=a[i]-e[i];f[i]:=a[i]-f[i];
od;
s:=sort([evalf(norm(b,frobenius)),evalf(norm(c,frobenius)),
evalf(norm(d,frobenius)),evalf(norm(e,frobenius)),
evalf(norm(f,frobenius))]);
if s[1]= evalf(norm(b,frobenius))
then print("Gruppo S(5)") fi;
if s[1]= evalf(norm(c,frobenius))
then print("Gruppo A(5)") fi;
if s[1]= evalf(norm(d,frobenius))
then print("Gruppo F(20)") fi;
if s[1]= evalf(norm(e,frobenius))
then print("Gruppo D(5)") fi;
if s[1]= evalf(norm(f,frobenius))
then print("Gruppo C(5)") fi;
end:

Chebotarev6:=proc(list,nu)
```

```
local i,dt11,dt10,dt9,dt8,dt7,dt6,dt5,
dt4,dt3,dt2,dt1,perc;
dt11:=0;dt10:=0;dt9:=0;dt8:=0;dt7:=0;dt6:=0;
dt5:=0;dt4:=0;dt3:=0;dt2:=0;dt1:=0;
for i from 1 to nu do
if member(6,list[i]) then dt11:=dt11+1 else
if verify(list[i],[0,1,5],sublist) then dt10:=dt10+1 else
if verify(list[i],[0,2,4],sublist) then dt9:=dt9+1 else
if verify(list[i],[0,1,1,4],sublist) then dt8:=dt8+1 else
if verify(list[i],[0,3,3],sublist) then dt7:=dt7+1 else
if verify(list[i],[0,1,2,3],sublist) then dt6:=dt6+1 else
if verify(list[i],[0,1,1,1,3],sublist)
then dt5:=dt5+1 else
if verify(list[i],[0,2,2,2],sublist) then dt4:=dt4+1 else
if verify(list[i],[0,1,1,2,2],sublist)
then dt3:=dt3+1 else
if verify(list[i],[0,1,1,1,1,2],sublist)
then dt2:=dt2+1 else
if verify(list[i],[0,1,1,1,1,1,1],sublist) then dt1:=dt1+1
fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;
od;
print((0,0,0,0,0,6)=dt11/nu);
print((0,0,0,0,1,5)=dt10/nu);
print((0,0,0,0,2,4)=dt9/nu);
print((0,0,0,1,1,4)=dt8/nu);
print((0,0,0,0,3,3)=dt7/nu);
print((0,0,0,1,2,3)=dt6/nu);
print((0,0,1,1,1,3)=dt5/nu);
print((0,0,0,2,2,2)=dt4/nu);
print((0,0,1,1,2,2)=dt3/nu);
print((0,1,1,1,1,2)=dt2/nu);
print((1,1,1,1,1,1)=dt1/nu);
perc:=array(1..nu,[dt1/nu,dt2/nu,dt3/nu,dt4/nu,
dt5/nu,dt6/nu,dt7/nu, dt8/nu,dt9/nu,dt10/nu,dt11/nu]);
getGroup6(perc);
end:

getGroup6:=proc(a)
local i,ss,b,c,d,e,f,g,h,ii,l,m,n,o,p,q,r,s;
b:=array(1..11,[1/720,15/720,45/720,15/720,40/720,120/720,
40/720,90/720,90/720,144/720,120/720]);
c:=array(1..11,[1/360,0,45/360,0,40/360,0,
40/360,0,90/360,144/360,0]);
d:=array(1..11,[1/120,0,15/120,10/120,0,0,
20/120,30/120,0,24/120,20/120]);
e:=array(1..11,[1/72,6/72,9/72,6/72,4/72,
12/72,4/72,0,18/72,0,12/72]);
f:=array(1..11,[1/60,0,15/60,0,0,0,20/60,0,0,24/60,0]);
g:=array(1..11,[1/48,3/48,9/48,7/48,0,0,
8/48,6/48,6/48,0,8/48]);
h:=array(1..11,[1/36,0,9/36,0,4/36,0,4/36,0,18/36,0,0]);
ii:=array(1..11,[1/36,0,9/36,6/36,4/36,0,
4/36,0,0,0,12/36]);
l:=array(1..11,[1/24,0,3/24,6/24,0,0,8/24,6/24,0,0,0]);
m:=array(1..11,[1/24,0,9/24,0,0,0,8/24,0,6/24,0,0]);
n:=array(1..11,[1/24,3/24,3/24,1/24,0,0,8/24,0,0,0,8/24]);
o:=array(1..11,[1/18,0,0,3/18,4/18,0,4/18,0,0,0,6/18]);
p:=array(1..11,[1/12,0,3/12,0,0,0,8/12,0,0,0,0]);
q:=array(1..11,[1/12,0,3/12,4/12,0,0,2/12,0,0,0,2/12]);
r:=array(1..11,[1/6,0,0,3/6,0,0,2/6,0,0,0,0]);
s:=array(1..11,[1/6,0,0,1/6,0,0,2/6,0,0,0,2/6]);
for i from 1 to 11 do
```

```
b[i]:=a[i]-b[i];c[i]:=a[i]-c[i]; d[i]:=a[i]-d[i];
e[i]:=a[i]-e[i];f[i]:=a[i]-f[i]; g[i]:=a[i]-g[i];
h[i]:=a[i]-h[i];ii[i]:=a[i]-ii[i];l[i]:=a[i]-l[i];
m[i]:=a[i]-m[i];n[i]:=a[i]-n[i];o[i]:=a[i]-o[i];
p[i]:=a[i]-p[i];q[i]:=a[i]-q[i];r[i]:=a[i]-r[i];
s[i]:=a[i]-s[i];
od;
ss:=sort([evalf(norm(b,frobenius)),
evalf(norm(c,frobenius)),
evalf(norm(d,frobenius)),evalf(norm(e,frobenius)),
evalf(norm(f,frobenius)),evalf(norm(g,frobenius)),
evalf(norm(h,frobenius)),evalf(norm(ii,frobenius)),
evalf(norm(l,frobenius)),evalf(norm(m,frobenius)),
evalf(norm(n,frobenius)),evalf(norm(o,frobenius)),
evalf(norm(p,frobenius)),evalf(norm(q,frobenius)),
evalf(norm(r,frobenius)),evalf(norm(s,frobenius))]);
if ss[1]= evalf(norm(b,frobenius))
then print("Gruppo S(6)") fi;
if ss[1]= evalf(norm(c,frobenius))
then print("Gruppo A(6)") fi;
if ss[1]= evalf(norm(d,frobenius))
then print("Gruppo PGL(2,5)") fi;
if ss[1]= evalf(norm(e,frobenius))
then print("Gruppo G(72)") fi;
if ss[1]= evalf(norm(f,frobenius))
then print("Gruppo PSL(2,5)") fi;
if ss[1]= evalf(norm(g,frobenius))
then print("Gruppo G(48)") fi;
if ss[1]= evalf(norm(h,frobenius))
then print("Gruppo G2(36)") fi;
if ss[1]= evalf(norm(ii,frobenius))
```

```
then print("Gruppo G1(36)") fi;
if ss[1]= evalf(norm(l,frobenius))
then print("Gruppo S(4)-") fi;
if ss[1]= evalf(norm(m,frobenius))
then print("Gruppo S(4)+") fi;
if ss[1]= evalf(norm(n,frobenius))
then print("Gruppo G(24)") fi;
if ss[1]= evalf(norm(o,frobenius))
then print("Gruppo G(18)") fi;
if ss[1]= evalf(norm(p,frobenius))
then print("Gruppo A(4)") fi;
if ss[1]= evalf(norm(q,frobenius))
then print("Gruppo D(6)") fi;
if ss[1]= evalf(norm(r,frobenius))
then print("Gruppo S(3))")fi;
if ss[1]= evalf(norm(s,frobenius))
then print("Gruppo C(6)")fi;
end:

Chebotarev7:=proc(list,nu)
local i,dt15,dt14,dt13,dt12,dt11,dt10,dt9,dt8,dt7,dt6,dt5,
dt4,dt3,dt2,dt1,perc;
dt15:=0;dt14:=0;dt13:=0;dt12:=0;dt11:=0;dt10:=0;dt9:=0;
dt8:=0;dt7:=0;dt6:=0;dt5:=0;dt4:=0;dt3:=0;dt2:=0;dt1:=0;
for i from 1 to nu do
if member(7,list[i]) then dt15:=dt15+1 else
if verify(list[i],[0,1,6],sublist) then dt14:=dt14+1 else
if verify(list[i],[0,2,5],sublist) then dt13:=dt13+1 else
if verify(list[i],[0,1,1,5],sublist)
then dt12:=dt12+1 else
if verify(list[i],[0,3,4],sublist)
```

```
then dt11:=dt11+1 else
if verify(list[i],[0,1,2,4],sublist)
then dt10:=dt10+1 else
if verify(list[i],[0,1,1,1,4],sublist)
then dt9:=dt9+1 else
if verify(list[i],[0,1,3,3],sublist)
then dt8:=dt8+1 else
if verify(list[i],[0,2,2,3],sublist)
then dt7:=dt7+1 else
if verify(list[i],[0,1,1,2,3],sublist)
then dt6:=dt6+1 else
if verify(list[i],[0,1,1,1,1,3],sublist)
then dt5:=dt5+1 else
if verify(list[i],[0,1,2,2,2],sublist)
then dt4:=dt4+1 else
if verify(list[i],[0,1,1,1,2,2],sublist)
then dt3:=dt3+1 else
if verify(list[i],[0,1,1,1,1,1,2],sublist)
then dt2:=dt2+1 else
if verify(list[i],[0,1,1,1,1,1,1,1],sublist)
then dt1:=dt1+1
fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi
od;
print((0,0,0,0,0,0,7)=dt15/nu);
print((0,0,0,0,0,1,6)=dt14/nu);
print((0,0,0,0,0,2,5)=dt13/nu);
print((0,0,0,0,1,1,5)=dt12/nu);
print((0,0,0,0,0,3,4)=dt11/nu);
print((0,0,0,0,1,2,4)=dt10/nu);
print((0,0,0,1,1,1,4)=dt9/nu);
print((0,0,0,0,1,3,3)=dt8/nu);
print((0,0,0,0,2,2,3)=dt7/nu);
print((0,0,0,1,1,2,3)=dt6/nu);
print((0,0,1,1,1,1,3)=dt5/nu);
print((0,0,0,1,2,2,2)=dt4/nu);
print((0,0,1,1,1,2,2)=dt3/nu);
print((0,1,1,1,1,1,2)=dt2/nu);
print((1,1,1,1,1,1,1)=dt1/nu);
perc:=array(1..nu,[dt1/nu,dt2/nu,dt3/nu,dt4/nu,dt5/nu,
dt6/nu,dt7/nu,dt8/nu,dt9/nu,dt10/nu,dt11/nu,dt12/nu,
dt13/nu,dt14/nu,dt15/nu]);
getGroup7(perc);
end:

getGroup7:=proc(a)
local i,s,b,c,d,e,f,g,h;
b:=array(1..15,[1/5040,21/5040,105/5040,105/5040,
70/5040,420/5040,210/5040,280/5040,210/5040,630/5040,
420/5040,504/5040,504/5040,840/5040,720/5040]);
c:=array(1..15,[ 1/2520,0,105/2520,0,70/2520,0,210/2520,
280/2520,0,630/2520,0,504/2520,0,0,720/2520]);
d:=array(1..15,[1/168,0,21/168,0,0,0,0,56/168,
0,42/168,0,0,0,0,48/168]);
e:=array(1..15,[1/42,0,0,7/42,0,0,0,14/42,0,0,
0,0,0,14/42,6/42]);
f:=array(1..15,[1/21,0,0,0,0,0,0,14/21,0,0,0,0,0,0,6/21]);
g:=array(1..15,[1/14,0,0,7/14,0,0,0,0,0,0,0,0,0,0,6/14]);
h:=array(1..15,[1/7,0,0,0,0,0,0,0,0,0,0,0,0,0,6/7]);
for i from 1 to 15 do
b[i]:=a[i]-b[i];c[i]:=a[i]-c[i]; d[i]:=a[i]-d[i];
e[i]:=a[i]-e[i];f[i]:=a[i]-f[i]; g[i]:=a[i]-g[i];
h[i]:=a[i]-h[i];
```

```
od;
s:=sort([evalf(norm(b,frobenius)),evalf(norm(c,frobenius)),
evalf(norm(d,frobenius)),evalf(norm(e,frobenius)),
evalf(norm(f,frobenius)), evalf(norm(g,frobenius)),
evalf(norm(h,frobenius))]);
if s[1]= evalf(norm(b,frobenius))
then print("Gruppo S(7)") fi;
if s[1]= evalf(norm(c,frobenius))
then print("Gruppo A(7)") fi;
if s[1]= evalf(norm(d,frobenius))
then print("Gruppo PSL(2,7)") fi;
if s[1]= evalf(norm(e,frobenius))
then print("Gruppo F(42)") fi;
if s[1]= evalf(norm(f,frobenius))
then print("Gruppo F(21)") fi;
if s[1]= evalf(norm(g,frobenius))
then print("Gruppo D(7)") fi;
if s[1]= evalf(norm(h,frobenius))
then print("Gruppo C(7)") fi;
end:


Chebotarev11:=proc(list,nu)
local i,dt,perc;
dt:=array(1..56,[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0]);
for i from 1 to nu do
if verify(list[i],[0,1,1,1,1,1,1,1,1,1,1,1],sublist)
then dt[1]:=dt[1]+1 else
if verify(list[i],[0,1,1,1,1,1,1,1,1,1,2],sublist)
```

```
then dt[2]:=dt[2]+1 else
if verify(list[i],[0,1,1,1,1,1,1,1,2,2],sublist)
then dt[3]:=dt[3]+1 else
if verify(list[i],[0,1,1,1,1,1,2,2,2],sublist)
then dt[4]:=dt[4]+1 else
if verify(list[i],[0,1,1,1,2,2,2,2],sublist)
then dt[5]:=dt[5]+1 else
if verify(list[i],[0,1,2,2,2,2,2],sublist)
then dt[6]:=dt[6]+1 else
if verify(list[i],[0,1,1,1,1,1,1,1,1,3],sublist)
then dt[7]:=dt[7]+1 else
if verify(list[i],[0,1,1,1,1,1,1,2,3],sublist)
then dt[8]:=dt[8]+1 else
if verify(list[i],[0,1,1,1,1,2,2,3],sublist)
then dt[9]:=dt[9]+1 else
if verify(list[i],[0,1,1,2,2,2,3],sublist)
then dt[10]:=dt[10]+1 else
if verify(list[i],[0,2,2,2,2,3],sublist)
then dt[11]:=dt[11]+1 else
if verify(list[i],[0,1,1,1,1,1,3,3],sublist)
then dt[12]:=dt[12]+1 else
if verify(list[i],[0,1,1,1,2,3,3],sublist)
then dt[13]:=dt[13]+1 else
if verify(list[i],[0,1,2,2,3,3],sublist)
then dt[14]:=dt[14]+1 else
if verify(list[i],[0,1,1,3,3,3],sublist)
then dt[15]:=dt[15]+1 else
if verify(list[i],[0,2,3,3,3],sublist)
then dt[16]:=dt[16]+1 else
if verify(list[i],[0,1,1,1,1,1,1,1,4],sublist)
then dt[17]:=dt[17]+1 else
```

```
if verify(list[i],[0,1,1,1,1,1,2,4],sublist)
then dt[18]:=dt[18]+1 else
if verify(list[i],[0,1,1,1,2,2,4],sublist)
then dt[19]:=dt[19]+1 else
if verify(list[i],[0,1,2,2,2,4],sublist)
then dt[20]:=dt[20]+1 else
if verify(list[i],[0,1,1,1,1,3,4],sublist)
then dt[21]:=dt[21]+1 else
if verify(list[i],[0,1,1,2,3,4],sublist)
then dt[22]:=dt[22]+1 else
if verify(list[i],[0,2,2,3,4],sublist)
then dt[23]:=dt[23]+1 else
if verify(list[i],[0,1,3,3,4],sublist)
then dt[24]:=dt[24]+1 else
if verify(list[i],[0,1,1,1,4,4],sublist)
then dt[25]:=dt[25]+1 else
if verify(list[i],[0,1,2,4,4],sublist)
then dt[26]:=dt[26]+1 else
if verify(list[i],[0,3,4,4],sublist)
then dt[27]:=dt[27]+1 else
if verify(list[i],[0,1,1,1,1,1,1,5],sublist)
then dt[28]:=dt[28]+1 else
if verify(list[i],[0,1,1,1,1,2,5],sublist)
then dt[29]:=dt[29]+1 else
if verify(list[i],[0,1,1,2,2,5],sublist)
then dt[30]:=dt[30]+1 else
if verify(list[i],[0,2,2,2,5],sublist)
then dt[31]:=dt[31]+1 else
if verify(list[i],[0,1,1,1,3,5],sublist)
then dt[32]:=dt[32]+1 else
if verify(list[i],[0,1,2,3,5],sublist)
```

```
then dt[33]:=dt[33]+1 else
if verify(list[i],[0,3,3,5],sublist)
then dt[34]:=dt[34]+1 else
if verify(list[i],[0,1,1,4,5],sublist)
then dt[35]:=dt[35]+1 else
if verify(list[i],[0,2,4,5],sublist)
then dt[36]:=dt[36]+1 else
if verify(list[i],[0,1,5,5],sublist)
then dt[37]:=dt[37]+1 else
if verify(list[i],[0,1,1,1,1,1,6],sublist)
then dt[38]:=dt[38]+1 else
if verify(list[i],[0,1,1,1,2,6],sublist)
then dt[39]:=dt[39]+1 else
if verify(list[i],[0,1,2,2,6],sublist)
then dt[40]:=dt[40]+1 else
if verify(list[i],[0,1,1,3,6],sublist)
then dt[41]:=dt[41]+1 else
if verify(list[i],[0,2,3,6],sublist)
then dt[42]:=dt[42]+1 else
if verify(list[i],[0,1,4,6],sublist)
then dt[43]:=dt[43]+1 else
if verify(list[i],[0,5,6],sublist)
then dt[44]:=dt[44]+1 else
if verify(list[i],[0,1,1,1,1,7],sublist)
then dt[45]:=dt[45]+1 else
if verify(list[i],[0,1,1,2,7],sublist)
then dt[46]:=dt[46]+1 else
if verify(list[i],[0,2,2,7],sublist)
then dt[47]:=dt[47]+1 else
if verify(list[i],[0,1,3,7],sublist)
then dt[48]:=dt[48]+1 else
```

```
if verify(list[i],[0,4,7],sublist)
then dt[49]:=dt[49]+1 else
if verify(list[i],[0,1,1,1,8],sublist)
then dt[50]:=dt[50]+1 else
if verify(list[i],[0,1,2,8],sublist)
then dt[51]:=dt[51]+1 else
if verify(list[i],[0,3,8],sublist)
then dt[52]:=dt[52]+1 else
if verify(list[i],[0,1,1,9],sublist)
then dt[53]:=dt[53]+1 else
if verify(list[i],[0,2,9],sublist)
then dt[54]:=dt[54]+1 else
if verify(list[i],[0,1,10],sublist)
then dt[55]:=dt[55]+1 else
if member(11,list[i])
then dt[56]:=dt[56]+1
fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;
fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;
fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;
fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;fi;
od;
for i from 1 to 56 do
perc[i]:=dt[i]/nu;
print(perc[i]);
od;
getGroup11(perc);
end:


getGroup11:=proc(a)
local i,s,b,c,d,e,f,g,h,l;
```

```
b:=array(1..56,[1/39916800, 1/725760, 1/40320, 1/5760,
1/2304, 1/3840, 1/120960, 1/4320, 1/576, 1/288, 1/1152,
1/2160, 1/216, 1/144, 1/324, 1/324, 1/20160, 1/960,
 1/192, 1/192, 1/288, 1/48, 1/96, 1/72, 1/192,
1/64, 1/96, 1/3600, 1/240, 1/80, 1/240, 1/90, 1/30,
1/90, 1/40, 1/40, 1/50, 1/720, 1/72, 1/48, 1/36, 1/36,
1/24, 1/30, 1/168, 1/28, 1/56, 1/21, 1/28, 1/48, 1/16,
1/24, 1/18, 1/18, 1/10, 1/11] );
c:=array(1..56,[1/19958400, 0, 1/20160, 0, 1/1152, 0,
1/60480, 0, 1/288, 0, 1/576, 1/1080, 0, 1/72, 1/162, 0,
0, 1/480, 0, 1/96, 0, 1/24, 0, 0, 1/96, 0, 1/48, 1/1800,
0, 1/40, 0, 1/45, 0, 1/45, 0, 1/20, 1/25, 0, 1/36, 0, 0,
1/18, 1/12, 0, 1/84, 0, 1/28, 2/21, 0, 0, 1/8, 0, 1/9, 0,
0, 2/11]);
d:=array(1..56,[1/7920, 0, 0, 0, 1/48, 0, 0, 0, 0, 0, 0,
0, 0, 0, 1/18, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1/8, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 1/5, 0, 0, 0, 0, 1/6, 0, 0, 0,
0, 0, 0, 0, 0, 1/4, 0, 0, 0, 0, 2/11]);
e:=array(1..56,[1/660, 0, 0, 0, 1/12, 0, 0, 0, 0, 0, 0,
0, 0, 0, 1/6, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 2/5, 0, 0, 0, 0, 1/6, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 2/11]);
f:=array(1..56,[1/110, 0, 0, 0, 0, 1/10, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 2/5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 2/5, 1/11]);
g:=array(1..56,[1/55, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 4/5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 2/11]);
h:=array(1..56,[1/22, 0, 0, 0, 0, 1/2, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 5/11]);
l:=array(1..56,[1/11, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 10/11]);
for i from 1 to 56 do
b[i]:=a[i]-b[i];c[i]:=a[i]-c[i]; d[i]:=a[i]-d[i];
l[i]:=a[i]-l[i];e[i]:=a[i]-e[i];f[i]:=a[i]-f[i];
g[i]:=a[i]-g[i]; h[i]:=a[i]-h[i];
od;
s:=sort([evalf(norm(b,frobenius)),evalf(norm(c,frobenius)),
evalf(norm(d,frobenius)), evalf(norm(e,frobenius)),
evalf(norm(f,frobenius)), evalf(norm(g,frobenius)),
evalf(norm(h,frobenius)), evalf(norm(l,frobenius))]);
if s[1]= evalf(norm(b,frobenius))
then print("Gruppo S(11)") fi;
if s[1]= evalf(norm(c,frobenius))
then print("Gruppo A(11)") fi;
if s[1]= evalf(norm(d,frobenius))
then print("Gruppo M(11)") fi;
if s[1]= evalf(norm(e,frobenius))
then print("Gruppo PSL(2,11)") fi;
if s[1]= evalf(norm(f,frobenius))
then print("Gruppo F(110)") fi;
if s[1]= evalf(norm(g,frobenius))
then print("Gruppo F(55)") fi;
if s[1]= evalf(norm(h,frobenius))
then print("Gruppo D(11)") fi;
if s[1]= evalf(norm(l,frobenius))
```

```
then print("Gruppo C(11)") fi;
end:


Chebotarev1:=proc(f,n)
local i,j,s,num,type,primes,dec,e;
s:=NULL;num:=0;
for i from 1 to n do
if isprime(i) then s:=s,i fi;
od;
primes:=[s];
primes;
dec:=NULL;
for i from 1 to nops(primes) do
if gcd(primes[i],discrim(f,x))=1 then num:=num+1;
dec:=dec,(Factor(f)mod primes[i]) fi;
od;
dec:=[dec];
for i from 1 to nops(dec) do
e:=array(1..degree(f));
e:=convert(dec[i],'list');
type[i]:=NULL;
for j from 1 to nops(e) do type[i]:=type[i],degree(e[j]) od;
type[i]:=sort([type[i]]);
od;
if degree(f)=3 then
Chebotarev3(type,num) else
if degree(f)=4 then
Chebotarev4(type,num) else
if degree(f)=5 then
Chebotarev5(type,num) else
```

```
if degree(f)=6 then
Chebotarev6(type,num) else
if degree(f)=7 then
Chebotarev7(type,num) else
if degree(f)=11 then
Chebotarev11(type,num)
fi;fi;fi;fi;fi;fi;
end:

Chebotarev:=proc(f,n)
if irreduc(f) then
Chebotarev1(f,n); print(galois(f)) else
print("Errore: il polinomio è riducibile!") fi;
end:
```

List of Tables

Bibliography

[BM83] Gregory Butler and John McKay. The transitive groups of degree up to 11. *Communications in Algebra*, 11:863–911, 1983.

[Bra86] Rolf Brandl. Integer polynomials that are reducible modulo all primes. *Amer. Math. Monthly*, 93(4):286–288, 1986.

[Bur55] W. Burnside. *Theory of groups of finite order.* Dover Publications Inc., New York, 1955. 2d ed.

[CHM98] John H. Conway, Alexander Hulpke, and John McKay. On transitive permutation groups. *j-LMS-J-COMPUT-MATH*, 1:1–8, 1998.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$.* A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[EFM79] D. W. Erbach, J. Fisher, and J. McKay. Polynomials with PSL(2, 7) as Galois group. *J. Number Theory*, 11(1):69–75, 1979.

[Jan96] Gerald J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, second edition, 1996.

[Jor72] C. Jordan. Recherches sur les substitutions. *Liouville Journal.*, 2(17):351–368, 1872.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[LN86] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, Cambridge, 1986.

[LN94] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, Cambridge, first edition, 1994.

[LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.

[LS91] H. W. Lenstra, Jr. and P. Stevenhagen. Primes of degree one and algebraic cases of Čebotarev's theorem. *Enseign. Math. (2)*, 37(1-2):17–30, 1991.

[McK79] J. McKay. Some remarks on computing Galois groups. *SIAM J. Comput.*, 8(3):344–347, 1979.

[MM97] Thomas Mattman and John McKay. Computation of Galois groups over function fields. *Math. Comp.*, 66(218):823–831, 1997.

[Rot95] Joseph J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.

[Šaf54] I. R. Šafarevič. Construction of fields of algebraic numbers with given solvable Galois group. *Izv. Akad. Nauk SSSR. Ser. Mat.*, 18:525–578, 1954.

[Sam67] Pierre Samuel. *Théorie algébrique des nombres.* Hermann, Paris, 1967.

[Ser92] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics.* Jones and Bartlett Publishers, Boston, MA, 1992. Lecture notes prepared by Henri Damon [Henri Darmon], With a foreword by Darmon and the author.

[Ser03] Jean-Pierre Serre. On a theorem of Jordan. *Bull. Amer. Math. Soc. (N.S.)*, 40(4):429–440 (electronic), 2003.

[SL96] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2):26–37, 1996.

[SM85] Leonard Soicher and John McKay. Computing Galois groups over the rationals. *J. Number Theory*, 20(3):273–281, 1985.

[ST02] Ian Stewart and David Tall. *Algebraic number theory and Fermat's last theorem.* A K Peters Ltd., Natick, MA, third edition, 2002.

[Sta73] Richard P. Stauduhar. The determination of Galois groups. *Math. Comp.*, 27:981–996, 1973.

[vdW91] B. L. van der Waerden. *Algebra. Vol. I.* Springer-Verlag, New York, 1991. Based in part on lectures by E. Artin and E. Noether, Translated from the seventh German edition by Fred Blum and John R. Schulenberger.

[Völ96] Helmut Völklein. *Groups as Galois groups*, volume 53 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 1996. An introduction.

[Wym72] B. F. Wyman. What is a reciprocity law? *Amer. Math. Monthly*, 79:571–586; correction, ibid. 80 (1973), 281, 1972.