

Classification Results for Intersective Polynomials With No Integral Roots

by

Nicolas Banks

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Pure Mathematics

Waterloo, Ontario, Canada, 2025

© Nicolas Banks 2025

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner: Karl Dilcher
Professor, Dept. of Mathematics & Statistics, Dalhousie University

Supervisor(s): David McKinnon
Professor, Dept. of Pure Mathematics, University of Waterloo

Internal Member: Xiaoheng Jerry Wang
Associate Professor, Dept. of Pure Mathematics,
University of Waterloo

Internal-External Member: Craig S. Kaplan
Professor, Cheriton School of Computer Science,
University of Waterloo

Other Member(s): Matthew Satriano
Associate Professor, Dept. of Pure Mathematics,
University of Waterloo

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

In this thesis, we algebraically classify strongly intersective polynomials - polynomials with no integer roots but with a root modulo every positive integer - of degrees 5–10. In particular, we compute a list of possible Galois groups of such polynomials. We also prove constraints on the splitting behaviour of ramified primes (i.e., primes that ramify in a splitting field of the polynomial). In the process, we show that intersectivity can be thought of as a property of a Galois number field, together with its set of subfields of specified degrees. This was achieved with characterisations of Berend-Bilu and Sonn, the latter of which we generalise. We also utilise Hensel’s Lemma and other standard results on the local behaviour of simple field extensions. Implementations in SageMath and GAP are provided.

Acknowledgements

I extend warm thanks to my supervisor, David McKinnon, for his unwavering support, patience, and dedication. I have learned many valuable lessons and skills from his guidance that will persist with me beyond my formal education.

I thank my supervisory committee, Yu-Ru Liu, Matt Satriano, and Jerry Wang, for their helpful comments and encouragement.

I thank my examining committee, Karl Dilcher, Craig Kaplan, Matt Satriano, and Jerry Wang, for their diligent proofreading and for helping turn my thesis into the best version of itself.

I thank my colleague, Bhawesh Mishra, for his thoughtful suggestions, insights, and encouragement.

I thank my dear friends and family for their support, distractions, and opportunities to bore them with mathematical jargon.

Finally, I lovingly thank my partner, Octavia. I will be striving for the rest of my life to embody the dedication, faith, and patience that you've shown me.

Table of Contents

Examining Committee Membership	ii
List of Tables	viii
List of Symbols	ix
1 Introduction	1
1.1 Contributions	1
1.2 History & Existing Literature	4
1.3 Ergodic Theory	12
1.4 A Word on Function Fields	15
2 Local Structure of Intersective Polynomials	17
2.1 p -Adic Roots	17
2.2 Decomposition Groups	20
3 The Galois Theory of Intersective Polynomials	23
3.1 Transitivity Degrees	23
3.2 Conjugate Covering	25
3.3 Subdirect Products	26
4 Possible Galois Groups of Strongly Intersective Polynomials	28
4.1 The Classification Theorem	28
4.2 Observations and Conjectures	30

References	33
APPENDICES	38
A Table of Subdirect Products for Products of Galois Groups	39
B Table of Transitive Subgroups That are Conjugate-Covered by Subgroups of Certain Indices	63
C Table of Possible Galois Groups of Strongly Intersective Polynomials	74
D Background	83
D.1 Algebraic Number Theory	83
D.2 Discriminants of Number Fields	91
D.3 Frobenius Elements of Number Fields	95
D.4 The p -Adic Integers and p -Adic Numbers	102
D.5 Finite Extensions of $\mathbb{Q}_p$	111
D.6 Extensions of the p -Adic Absolute Value	116

List of Tables

A.1	Proper subdirect products of direct products of Galois groups of degrees 5 to 10	39
B.1	Transitive groups of certain degrees which can be conjugate-covered by subgroups of given indices	63
C.1	Possible Galois groups of strongly intersective polynomials of degrees 5 to 10, with some examples	74

List of Symbols

$\mathbb{Z}_p$	The integral domain of p -adic integers, where p is a prime number.
$R[x_1, \dots, x_k]$	The polynomial ring in the variables $x_1, \dots, x_k$ with coefficients in R , where R is a ring.
$\mathfrak{p}, \mathfrak{q}$	A non-zero prime ideal of some ring of integers or valuation ring $\mathcal{O}_L$. Usually we simply call these <i>primes of L</i> .
$F(\alpha_1, \dots, \alpha_n)$	The smallest field extension of F containing $\alpha_1, \dots, \alpha_n$, where F is a field and α_i algebraic over F . When $n = 1$, a more intrinsic definition is given by $F[x]/\langle f(x) \rangle$, where $f(x) \in F[x]$ is irreducible and depends on $\alpha := \alpha_1$; in this case, the class of x in this quotient ring behaves like a root of $f(x)$ and can be identified with α .
$\mathbb{Q}_p$	The field of p -adic numbers, where p is a prime number.
$\langle a \rangle, \text{ aR}$	The principal ideal of all R -multiples of a , where R is a ring and $a \in R$. Care must be taken when R is non-commutative and / or non-unital, which does not arise in the present work.
$[L : K]$	The degree of the field extension L/K , i.e., the dimension of L as a K -vector space with scalar multiplication defined simply as field multiplication in L .
$e_L(\mathfrak{p} \mid p), e(\mathfrak{p} \mid p), e$	The ramification degree of $\mathfrak{p}$ lying over p , where $\mathfrak{p}$ is a prime of L and L is either a number field or a p -adic field. The shorter notations are used when context eliminates the risk of confusion.

$f_L(\mathfrak{p} \mid p), f(\mathfrak{p} \mid p), f$	The inertia degree of $\mathfrak{p}$ lying over p . Like ramification degrees, the notation used depends on context and the required specificity.
$D_L(\mathfrak{p} \mid p), D(\mathfrak{p} \mid p)$	The decomposition group of $\mathfrak{p}$ lying over p , where L is a number field.
$\text{Gal}(K/F)$	Galois group of the field extension K/F . This notation is reserved for the case where K/F is a Galois extension. Otherwise, $\text{Aut}(K/F)$ is used.
$\text{Gal}(P(x)/F)$	Galois group of $P(x) \in F[x]$, defined as the Galois group of a splitting field of P over F .
$f'(x)$	The formal derivative of $f(x) \in R[x]$, where R is an integral domain. The definition is identical to the “power rule” from analysis.
$\text{disc}(P)$	The discriminant of $P(x) \in \mathbb{Z}[x]$, which is an integer; this is non-zero precisely when P is square-free in $\mathbb{Q}[x]$.
$\text{Res}(P, Q)$	The resultant of $P(x)$ and $Q(x) \in \mathbb{Z}[x]$, which is an integer; this is non-zero precisely when P and Q are relatively prime in $\mathbb{Q}[x]$.
$\text{rad}(n)$	The radical of n , where n is an integer, defined as the product of distinct prime factors of n .
$\langle a_1, \dots, a_n \rangle$	If $a_1, \dots, a_n \in R$ for a ring R , then this denotes the ideal of R generated by the a_i . When R is commutative and unital, as is always the case in the present work, this can be written as $\{\sum_{i=1}^n r_i a_i : r_i \in R\}$, i.e., the set of all finite R -linear combinations of elements of the generating set.
$\text{Ind}_H^G \rho$	The induced representation on G , where G is a group, H is a subgroup of G , and ρ is a representation of H . Note that this preserves the base field of the representation ρ .
$A \otimes_R B$	The tensor product of A and B over R , where R is a ring and A and B are R -modules.
$\left(\frac{a}{p}\right)$	The Legendre symbol of a modulo p , where a is an integer and p is an odd prime number.
S_n	Symmetric group of order $n!$.
C_n	Cyclic group of order n with multiplicative notation.
$\mathbb{Z}_{>0}$	The set of positive integers, which is used to avoid the controversial symbol $\mathbb{N}$.

$\mathbb{F}_q$	The finite field with q elements, where q is necessarily a power of a prime. When q is a prime, this is isomorphic to $\mathbb{Z}/q\mathbb{Z}$.
$\mathbb{F}_q(T)$	Rational functions in the variable T with coefficients in $\mathbb{F}_q$, i.e., the field of fractions of the polynomial ring $\mathbb{F}_q[T]$.
$\mathcal{O}_L$	If L is a number field, then this denotes its ring of integers. If L is a p -adic field, then this denotes its valuation ring.
$ \cdot _p$	The p -adic absolute value, where $p \in \mathbb{Z}$ is a prime number.
$L_{\mathfrak{p}}, \widehat{L}$	The metric completion of L with respect to the absolute value defined by $\mathfrak{p}$, where L is a number field and $\mathfrak{p}$ is a prime of L . The notation used depends on the risk of confusion with respect to the exact prime ideal that was used.
$\text{Frob}_L(\mathfrak{p} \mid p), \text{Frob}(\mathfrak{p} \mid p)$	The Frobenius element of $\mathfrak{p}$ over p in L , where $L/\mathbb{Q}$ is a number field and $\mathfrak{p}$ is a prime of L lying over the rational prime p .
D_n	Dihedral group of order $2n$, which can be constructed as the symmetries of a regular n -gon.
$G_1 : G_2$	A semidirect product $G_1 \rtimes_{\varphi} G_2$ of groups G_1 and G_2 , which depends on the homomorphism $\varphi : G_2 \rightarrow \text{Aut}(G_1)$, i.e., an action of G_2 on G_1 . Note that this notation suppresses the choice of action, so there may be several non-isomorphic groups with the name $G_1 : G_2$. Group IDs are given to distinguish these.
A_n	Alternating group of order $\frac{n!}{2}$.
F_n	Frobenius group of order $n(n-1)$. When n is prime, this can be constructed as a semidirect product $C_n : C_{n-1}$.
$G_1 \wr G_2$	A wreath product of groups G_1 and G_2 . This is defined as some semidirect product of a direct product of G_1 on G_2 , i.e., $(G_1^n) : G_2$ for some $n \geq 1$.
$\text{GL}(n, R)$	General linear group. The multiplicative group of invertible $n \times n$ -matrices with entries in the ring R . If R is given as a number instead, e.g., $\text{GL}(4, 2)$, then the entries are in a finite field of that size.

$\mathrm{SL}(n, R)$	Special linear group. The subgroup of $\mathrm{GL}(n, R)$ of matrices with determinant 1.
$\mathrm{SO}^+(2n, q)$	Special orthogonal group. “Orthogonal” means all matrices preserving a certain non-degenerate quadratic form. In even degree over finite fields, the $^+$ signifies a particular quadratic form, of which there are exactly two inequivalent choices.
$\mathrm{PGL}(n, q)$	Projective general linear group. The quotient of $\mathrm{GL}(n, q)$ by its centre, which turns out to be the set of scalar multiples of the identity matrix I .
$\mathrm{PGO}^+(2n, q)$	Projective general orthogonal group.
$\mathrm{PSO}^+(2n, q)$	Projective special orthogonal group.
Q_8	Quaternion group of order 8. This can be constructed as $\{\pm 1, \pm i, \pm j, \pm k\}$ satisfying the standard non-commutative quaternion relations, e.g., $ij = k$ and $ji = -k$.
$\mathrm{OD}_{2^n}, \mathrm{M}_{2^n}$	Modular maximal-cyclic group of order 2^n . This can be constructed as a semidirect product $C_{2^{n-1}} : C_2$. Note that the dihedral group $D_{2^{n-1}}$ can be constructed in a similar way, but they are not isomorphic, as the actions underlying the two semidirect product structures are different.
SD_{2^n}	Semidihedral group of order 2^n . This is yet another distinct semidirect product $C_{2^{n-1}} : C_2$, like $D_{2^{n-1}}$ and OD_{2^n} . In fact, these three families account for all possible such semidirect products, i.e., all possible actions of C_2 on $C_{2^{n-1}}$.
$\mathrm{disc}(L)$	The discriminant of the number field L ; this is always a non-zero, non-unit in $\mathbb{Z}$.
$I_L(\mathfrak{p} \mid p), I(\mathfrak{p} \mid p)$	The inertia group of $\mathfrak{p}$ lying over p , where L is a number field.

Chapter 1

Introduction

In Section 1.1, we introduce strongly intersective polynomials and state our novel results. In Section 1.2, we review the existing literature, including Galois-theoretic and number-theoretic characterisations. In Section 1.3, we discuss the origins of the subject in ergodic theory. In Section 1.4, we connect our work with similar questions over function fields.

1.1 Contributions

Throughout, let $p \in \mathbb{Z}$ be a prime number.

Since the success of the Hasse-Minkowski Theorem in the 1920s, which concerns solutions of quadratic forms, number theorists tend to approach problems with a local-global philosophy: To study a problem (e.g., to prove a theorem or to prove that a family of objects has a certain property) in $\mathbb{Z}$, it suffices to study the same problem in $\mathbb{R}$ and in all $\mathbb{Z}_p$, where $\mathbb{Z}_p$ is the integral domain of p -adic integers.

This approach has had many successes, notably including the modern approach to Class Field Theory. Therefore, it is very interesting to find situations where the local-global principle fails.

This thesis focuses on the local-global principle of the existence of polynomial roots, particularly the class of polynomials that violate this principle.

Definition 1.1.1. A polynomial $P \in \mathbb{Z}[x]$ is called **intersective** if it has a root modulo m for all positive integers m . We call P **strongly intersective** if it is intersective and has no roots in $\mathbb{Z}$. We call P **minimally (strongly) intersective** if no non-constant, proper divisor of P is (strongly) intersective.

Note that by the Chinese Remainder Theorem, having a root modulo m for all positive integers m is equivalent to having a root modulo all powers of all primes, and this in turn is equivalent to having a root in the p -adic integers $\mathbb{Z}_p$ for all primes p (see Theorem D.4.1).

The name “intersective” will be explained in Section 1.3.

Of course, a polynomial with an integer root is automatically intersective, so the strongly intersective ones are more interesting.

Strongly intersective polynomials may appear to only represent a “near” local-global failure, since no constraints are placed on roots lying in $\mathbb{R}$, the remaining completion associated with $\mathbb{Z}$ and $\mathbb{Q}$. However, a pre-print of Angelo and Xu [1, Theorem 1.1] shows via Chebotarev’s Density Theorem (see Theorem D.3.1) that intersective polynomials - in fact, polynomials with roots modulo all “large” primes - automatically have a real root.

An observation that we make in Section 2.1 is that intersectivity can be thought of as a field-theoretic property. More specifically, we prove

Corollary 1.1.1. *Let $P(x) = h_1(x) \cdots h_r(x) \in \mathbb{Z}[x]$ be factored into irreducibles. Then P is intersective if and only if, for each rational prime p , there is an i , a root θ_i of h_i , and a prime $\mathfrak{p}_i$ of $\mathbb{Q}(\theta_i)$ above p such that the completion of $\mathbb{Q}(\theta_i)$ at $\mathfrak{p}_i$ is isomorphic to $\mathbb{Q}_p$.*

In particular, for two such polynomials $P = h_1 \cdots h_r$ and $P' = h'_1 \cdots h'_r$ with $\deg(h_i) = \deg(h'_i)$, if each element of the set $\{\mathbb{Q}[x]/\langle h_i(x) \rangle\}$ is isomorphic to an element of $\{\mathbb{Q}[x]/\langle h'_j(x) \rangle\}$ and vice versa, then the intersectivity of P and P' is equivalent.

A theme of this thesis is also a theme in general algebraic number theory: Different tools are required to study behaviour at ramified and unramified primes. For example, using the same techniques, we prove a variant of the above in Section 2.1 involving splitting patterns of ramified primes in extensions generated by single roots:

Corollary 1.1.2. *Let $f \in \mathbb{Q}[x]$ be irreducible of degree ≥ 2 with root θ , Galois group G over $\mathbb{Q}$, and $n = [L : \mathbb{Q}] = |G| \geq 2$. Let p be a rational prime which ramifies in $\mathbb{Q}(\theta)$, and $\mathfrak{p}$ a prime of $\mathbb{Q}(\theta)$ above p . Then θ embeds into $\mathbb{Q}_p$ as a root of f via the embedding defined by $\mathfrak{p}$ if and only if the ramification and inertia degrees $e(\mathfrak{p}/p)$ and $f(\mathfrak{p}/p)$ of $\mathfrak{p}$ over p are both 1.*

More generally, let $P(x) = h_1(x) \cdots h_r(x) \in \mathbb{Q}[x]$ be factored into irreducibles, and let p be a rational prime which is ramified in a splitting field of P over $\mathbb{Q}$. Then P has a root in $\mathbb{Q}_p$ if and only if, for some $1 \leq i \leq r$, there is a root θ_i of h_i such that one of the primes of $\mathbb{Q}(\theta_i)$ above p has ramification and inertia degrees equal to 1.

This constitutes an algorithm for checking intersectivity at ramified primes, of which we give an implementation in SageMath.

Sonn [61] proved the following characterisation in 2008 in the course of studying the inverse Galois theory of intersective polynomials:

Theorem 1.1.1. [61, Proposition 1] *Let $L/\mathbb{Q}$ be a finite Galois extension with Galois group G . The following are equivalent:*

1. *L is the splitting field of a product $P = h_1 \cdots h_r$ of irreducible polynomials of degree greater than 1 in $\mathbb{Q}[x]$, and P has a root in $\mathbb{Q}_p$ for all primes p .*
2. *G is the union of the conjugates of r proper subgroups $H_1, \dots, H_r$, the intersection of all these conjugates is trivial, and for all primes $\mathfrak{p}$ of L , the decomposition group $D_L(\mathfrak{p} \mid p)$ is contained in a conjugate of some H_i .*

In Section 2.2, we prove that the second condition of the preceding theorem need only hold for primes of L which lie above ramified rational primes, which makes an algorithm out of Sonn's condition:

Theorem 1.1.2. *Let $L/\mathbb{Q}$ be a finite Galois extension with Galois group G . The following are equivalent:*

- (1) *L is the splitting field of a product $P = h_1 \cdots h_r$ of irreducible polynomials of degree greater than 1 in $\mathbb{Q}[x]$, and P has a root in $\mathbb{Q}_p$ for all primes p .*
- (2) *G is the union of the conjugates of r proper subgroups $H_1, \dots, H_r$, the intersection of all these conjugates is trivial, and for all primes $\mathfrak{p}$ of L lying over a ramified prime $p \in \mathbb{Z}$, the decomposition group $D_L(\mathfrak{p} \mid p)$ is contained in a conjugate of some H_i .*

The existing classification theorems for strongly intersective polynomials in the literature, as described in Section 1.2, are either non-constructive or utilise elementary number-theoretic methods. One of our main contributions is the following classification theorem, proved in Section 4.1, which uses sophisticated methods from algebraic number theory and Galois theory to achieve more general, yet still concrete, results.

Theorem 1.1.3. *Let P be a strongly intersective polynomial with Galois group G over $\mathbb{Q}$. If $5 \leq \deg(P) \leq 10$, then G must be one of the groups appearing in Table C.1.*

Moreover, as explained in Section 1.2, there are simple algebraic constraints on the Galois groups of strongly intersective polynomials which facilitate the following, proved in Section 3.3:

Corollary 1.1.3. *Let $P(x) = h_1(x) \cdots h_r(x)$ be factored into irreducibles over $\mathbb{Z}$. If $|\text{Gal}(h_i(x)/\mathbb{Q})|$ are all coprime, then $P(x)$ is not intersective.*

We will use this and other algebraic constraints sequentially in Section 4.1 to produce our Table C.1. We also discuss the process of finding examples corresponding to each possible Galois group. In particular, if a reducible polynomial has an appropriate Galois group, then there seem to be no obstructions to finding specific coefficients that achieve intersectivity. However, this is still conjectural.

Later in Section 4.1, we demonstrate how knowledge of the subgroup diagram of a particular group from Table C.1 can be coupled with Corollary 1.1.2 to construct explicit examples.

Finally, in Section 4.2, we discuss some consequences of Theorem 1.1.3, both proved and conjectural. The most concrete among these are the following:

Corollary 1.1.4. *Let $n \geq 7$ be odd. Then there is no strongly intersective polynomial of degree n whose factorisation shape is $(2, n-2)$ and whose Galois group is S_{n-2} .*

Conjecture 1.1.1. *Let $n \geq 6$ be even. Then there is no strongly intersective polynomial of degree n with factorisation shape $(2, n-2)$.*

1.2 History & Existing Literature

Deciding on the (strong) intersectivity of an arbitrary polynomial goes back to, at least, Ax in 1967, who gave a general recursive algorithm of a geometric flavour to determine if a system of multivariate Diophantine polynomials has a solution modulo all primes [4, Section 2]. This was followed nine years later by Fried and Sacerdote [29], whose algorithm is primitive recursive. We will not describe these results in more detail, although we contrast them to both the non-existence of such an algorithm over $\mathbb{Z}$, and the relative simplicity of Berend and Bilu’s result, stated presently.

In 1996, Berend and Bilu [7] provided a characterisation of single-variable intersective polynomials, which constitutes a simple and purely number-theoretic algorithm. It is now helpful to introduce Hensel’s Lemma.

Together with Krasner’s Lemma (Theorem D.6.1), Hensel’s Lemma is one of the only results directly connecting the algebra and topology of a field equipped with a discrete valuation. For better or worse, the name “Hensel’s Lemma” is given to many different results - in fact, we state a different version as background material in Appendix D.6, Theorem D.6.1 - so it is pertinent to be specific now:

Theorem 1.2.1 (Hensel’s Lemma). [54, Theorem 2.24] Let p be a prime number, $P(x) \in \mathbb{Z}[x]$, and $k \geq 0$. If P has a root a_k modulo p^k , and k is sufficiently large compared to the power of p which divides $P'(a_k)$, then there is a root a_{k+1} of P modulo p^{k+1} . Explicitly, suppose that p^v exactly divides $P'(a_k)$ and that $k \geq 2v + 1$. If $b \equiv a_k \pmod{p^{k-v}}$, then $P(b) \equiv P(a_k) \pmod{p^k}$ and p^v exactly divides $P'(b)$. Moreover, there is a unique t modulo p such that $P(a_k + tp^{k-v}) \equiv 0 \pmod{p^{k+1}}$.

Now for Berend and Bilu’s characterisation: Let $P(x) = h_1(x) \cdots h_r(x)$ be the factorisation of P into irreducibles over $\mathbb{Z}$. Also, assume that the coefficients of P are coprime (we can arrange for this by dividing by GCDs, which does not change the following results).

The algebraic setup is as follows: Let L be a splitting field of P over $\mathbb{Q}$, $G = \text{Gal}(L/\mathbb{Q})$, θ_i a fixed root of h_i , $K_i = \mathbb{Q}(\theta_i)$, $H_i = \text{Aut}(L/K_i) \leq G$, and $U = \bigcup_{i=1}^r H_i \subseteq G$.

Now for the arithmetic setup: Let $\delta_i = \text{disc}(h_i)$, $\rho_i = \text{Res}(h_i, h'_i)$, $\delta = \rho_1 \cdots \rho_r = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ the prime factorisation of δ , and finally, $\Delta = \delta^2 \text{rad}(\delta) = p_1^{2\alpha_1+1} \cdots p_s^{2\alpha_s+1}$.

Theorem 1.2.2. [7, Theorem 1] The following are equivalent:

1. P is intersective.
2. P has a root mod Δ , and

$$\bigcup_{\sigma \in G} \sigma^{-1} U \sigma = G \tag{1.1}$$

Remark 1. Some observations on this remarkable theorem:

- Sonn’s characterisation, Theorem 1.1.1, provides an alternative which does not involve finding polynomial roots.
- The prime powers of Δ are chosen so that Theorem 1.2.1 applies. Actually, instead of the resultant $\rho_i = \text{Res}(h_i, h'_i)$ used to define Δ , one can use the “reduced resultant” or “congruence number” of h_i , defined as the positive generator of the ideal $\langle h_i(x), h'_i(x) \rangle \cap \mathbb{Z}$ [55, the definition preceding Lemma 2.1].
- The proof shows that Condition (1.1) is equivalent to having roots modulo primes that do not divide $\text{disc}(P)$ (actually, primes that are unramified in $L/\mathbb{Q}$). In contrast, the ramified primes - the arithmetic information of P - is encapsulated in the number Δ .

- There are two ways to understand why taking conjugates is necessary to cover G . The first is that, since each subgroup comprising U is generated by a single root, the conjugation recovers the rest of the roots, i.e., their Galois conjugates in L . The second viewpoint, which is equivalent in some sense, is that Frobenius elements of number fields are only defined up to conjugation; see Appendix D.3 for background information on this.

There are some easy consequences of this characterisation, which were observed by Berend and Bilu in the same paper:

Corollary 1.2.1. *Let $P \in \mathbb{Z}[x]$.*

1. *If P is strongly intersective, then P must be reducible over $\mathbb{Q}$.*
2. *If P is strongly intersective, then $\deg(P) \geq 5$.*

This motivates the following definition:

Definition 1.2.1. Let G be a finite group with subgroups $H_1, \dots, H_r$. We say that G is **conjugate-covered by the H_i** if

$$G = \bigcup_{\sigma \in G} \bigcup_{i=1}^r \sigma^{-1} H_i \sigma.$$

Thus, Condition (1.1) says that G is conjugate-covered by r subgroups which correspond to subgroups fixing a particular root of each h_i , and strong intersectivity insists that the H_i are proper.

In fact, the number-theoretic context provides more insight into this condition. Let $L/\mathbb{Q}$ be a splitting field of $P \in \mathbb{Z}[x]$. In the course of proving Condition (1.1), Berend and Bilu show [7, Lemma 2] that P having a root modulo powers of an unramified (in L) rational prime p is equivalent to one of the Frobenius elements of p in L being in one of the H_i .

The problem of conjugate-covers of groups, and more generally of covering groups by k proper subgroups, has a rich history; see Bhargava [10] for a survey. In particular, groups that are minimally covered by 3 proper subgroups were completely characterised by Scorza in 1926 (c.f., the entirety of Scorza [58] for the original Italian, and Bruckheimer, Bryan, and Muir [12, Theorem 1] for an English proof), and analogous results were obtained by John H. E. Cohn in 1994 for 4, 5, and 6 proper subgroups [17, Theorem 5]. Surprisingly,

Tomkinson showed in 1997 that a covering by 7 proper subgroups is never minimal [65, Theorem 3.6].

Unfortunately, most results of this nature do not apply to this thesis. Many are either asymptotic in nature or are concerned with minimal (conjugate-)covering numbers. Our situation demands results that can produce multiple covering numbers for a given group, or properties that a family of subgroups must satisfy in order to cover the ambient group. Results of Brodie, Chamberlain, and Kappe, which concern the case of normal subgroups, appear to come closest to meeting our requirements [11, Theorem 1 & Corollary 3].

Interestingly, this work connects with character theory via Artin's Theorem on Induced Characters, also called Artin's Induction Theorem:

Definition 1.2.2. Let G be a finite group with subgroup H , and let (ρ, V) be a finite-dimensional K -representation of H for some field K . Then V can be viewed as a $K[H]$ -module, where $K[H]$ denotes the group ring over K generated by H . The **induced representation on G** is defined as

$$\text{Ind}_H^G \rho := K[G] \otimes_{K[H]} V,$$

which indeed is a $K[G]$ -module, i.e., a K -representation of G .

Intuitively, induced representations are the universal way to lift representations from subobjects to the ambient object.

Theorem 1.2.3 (Artin's Theorem on Induced Characters Theorem). [59, Theorem 17], [39, Theorem 3.3.2] *Let G be a finite group, and X a family of subgroups of G . The following are equivalent:*

1. G is conjugate-covered by the members of X , i.e.,

$$G = \bigcup_{\sigma \in G} \bigcup_{H \in X} \sigma^{-1} H \sigma.$$

2. Every finite-dimensional, complex character of G is a rational linear combination of characters induced by the members of X .

Note that this theorem is often stated in the particular case where X is the set of cyclic subgroups of G ; see a comprehensive reference on character theory like Isaacs [40, Theorem 5.21].

Sadly, a common sentiment among both representation theorists and number theorists is that Artin's theorem was superseded by Brauer's Theorem on Induced Characters, also called Brauer's Induction Theorem:

Definition 1.2.3. Let G be a finite group, and p a prime divisor of $|G|$. A subgroup of G is called a **p -elementary subgroup of G** if it is a direct product of a p -group and a cyclic group whose order is coprime to p . A subgroup of G which is p -elementary for some prime p is called an **elementary subgroup of G** .

Theorem 1.2.4 (Brauer's Theorem on Induced Characters). *[40, Theorem 8.4] Let G be a finite group. Then every finite-dimensional, complex character of G is an integer linear combination of 1-dimensional characters induced by elementary subgroups of G .*

Brauer's Theorem is interesting in its own right, but only generalises Artin's Theorem when we have restricted the latter to the set of cyclic subgroups of G . The general case of Artin's Theorem seems more applicable to the present context, and indeed, the application of character theory to interseptive polynomials seems to be completely open. There is, of course, a long history of applying character theory (and representation theory more broadly) to the study of finite groups, from Frobenius's Theorem on derangement subgroups [34, Theorem 4.5.1] to Burnside's Theorem on solvable groups [23, Theorem 19.2.1] to the entirety of the classification of finite simple groups [33].

Along more group theoretic lines, we mention some interesting connections with the theory of derangements:

Definition 1.2.4. Let a finite group G be embedded as a permutation group of degree n . A **derangement of G** is an element of G with no fixed points. In other words, $\sigma \in G$ is a derangement if $\sigma(i) \neq i$ for all $1 \leq i \leq n$.

To relate this to our standard set-up, let $P(x)$ be a possibly reducible polynomial over $\mathbb{Z}$, and let $L/\mathbb{Q}$ be a splitting field of P . If p is a rational prime which is unramified in $L/\mathbb{Q}$, then the Frobenius elements of p have cycle types corresponding to the factorisation of $P(x)$ modulo p (by applying Proposition D.3.4 factor-by-factor). Since every element of $\text{Gal}(P/\mathbb{Q})$ has the cycle type of some such Frobenius element by the Chebotarev Density Theorem (Theorem D.3.1 and Corollary D.3.2), Condition (1.1) is equivalent to every element of G having a fixed point (note, this was also observed by Elsholtz, Klahn, and Technau [26, preceding Proposition 2.2]). In other words, if P is interseptive, then G contains no derangements with respect to its action on the roots of P .

An elementary consequence of the Orbit-Stabiliser Theorem says that, if G acts transitively on a set Ω , then G contains a derangement. A much deeper result of Fein, Kantor,

and Schacher [28, Theorem 1] states that, in fact, G contains a derangement of prime-power order; there is no known proof of this fact that does not use the Classification of Finite Simple Groups. Of course, in our context the Galois group of a reducible polynomial does not act transitively on its roots, but it seems feasible in future work to apply this theorem factor-by-factor on the irreducible factors of such a polynomial.

The most recent results regarding conjugate-covering of groups appear to be a preprint by Ellis and Harper [25]. For example, their Theorem 3 states that if H_1 and H_2 are subgroups of a finite group G such that H_1 is proper, H_2 is maximal, and $|H_2|$ divides $|H_1|$, then G cannot be conjugate-covered by H_1 and H_2 . Additional results by Ellis and Harper of this nature include Corollaries 4 and 5 and the subsequent Remarks. These results are either conjectural or too specific to meaningfully simplify our calculations, but on the other hand, the methods of this thesis provide support for those conjectures; see Section 3.2 and Table B.1.

In the aforementioned paper from 2008 [61], Sonn gave a non-constructive proof that every finite solvable group which is the conjugate-union of some proper subgroups is the Galois group of an intersective polynomial, provided that these conjugates intersect trivially. The result was also proved for Frobenius groups in the case of two proper subgroups, i.e., $r = 2$. The next year, Sonn connected the case of non-solvable groups to the general inverse Galois problem over $\mathbb{Q}$ [62], and also gave a call for more examples of strongly intersective polynomials.

In 2013, Soule [63] studied polynomials with roots modulo prime powers for potentially small sets of primes, and classified certain families. For example, they showed that $\sum_{j=1}^{L-1} x^j$ has a root modulo all powers of primes that are congruent to 1 modulo L .

In the same year, Hyde and Spearman [38] classified intersective polynomials of degree 6 of a specific form:

Theorem 1.2.5. [38, Theorem 2.1] *Let $a, b > 1$ be square-free such that ab is not a perfect square. Let $\ell = \gcd(a, b)$, $a' = \frac{a}{\ell}$, and $b' = \frac{b}{\ell}$. Then the sextic*

$$P(x) = (x^2 - a)(x^2 - b)(x^2 - a'b')$$

is strongly intersective if and only if at least one of a , b , and $a'b'$ is 1 modulo 8, and for every odd prime p , at least one of the Legendre symbols

$$\left(\frac{a}{p}\right), \left(\frac{b}{p}\right), \text{ and } \left(\frac{a'b'}{p}\right)$$

has the value +1.

A year later, Hyde, Lee, and Spearman [37] classified another family of intersective polynomials, this time in degree 5:

Theorem 1.2.6. [37, Theorem 1] *Let $n \neq 1$ be cube-free. Then the quintic*

$$P(x) = (x^3 - n)(x^2 + 3)$$

is strongly intersective if and only if $n \equiv 1 \pmod{9}$ and all the prime factors of n are congruent to 1 modulo 3.

In 2022, Mishra [48] extended Theorem 1.2.5 to arbitrarily long products of quadratics, and moreover, the coefficients can be chosen so that the resulting polynomial is minimally strongly intersective. The algorithm to generate the coefficients rests on the following from Mishra's earlier work [49]:

Theorem 1.2.7. [49, Theorem 1] *Let $a_1, \dots, a_n$ be at least 3 distinct square-free integers, none equal to 1. Then the polynomial $P(x) = (x^2 - a_1)(x^2 - a_2) \cdots (x^2 - a_n)$ is strongly intersective if and only if the following are satisfied:*

1. *There exists a subset $T \subseteq \{1, 2, \dots, n\}$ of odd cardinality such that*
 - (a) *the product $\prod_{j \in T} a_j$ is a perfect square, and*
 - (b) *for every $j \in T$ and for every odd prime p dividing a_j , there exists $i \in \{1, \dots, n\}$, $i \neq j$, such that a_i is a square modulo p .*
2. *One of the a_k is 1 modulo 8.*

Also in 2022, Mishra generalised Berend and Bilu's results to arbitrary global fields [50, Theorem 1]. We explain the relationship between this thesis and these results in Section 1.4.

In the same year, Elsholtz, Klahn, and Technau [26] applied similar techniques to Berend and Bilu to investigate *exceptional polynomials*, i.e., polynomials with roots modulo all but finitely many primes. As an application, they classified irreducible polynomials h for which there exists an irreducible quadratic g such that hg is exceptional. This result suggests future work classifying the possible factorisations of intersective polynomials. They also classified exceptional polynomials whose irreducible factors were all of the form $x^p - a$ for a fixed prime p .

We now describe the existing algebraic tools that will facilitate the proof of our classification Theorem 1.1.3.

First, using the theory of resultants [3], G must be a subgroup of $S_1 \times \cdots \times S_r$ that is also a transitive subgroup of some S_d , where d is a multiple of $\text{lcm}(\deg(h_1), \dots, \deg(h_r))$ and a divisor of $\prod_{i=1}^r \deg(h_i)$. For example, in the case of a sextic which factors as a product of three irreducible quadratics, G must be a subgroup of C_2^3 which is also a transitive subgroup of C_2 , S_4 , or S_8 .

Unless n is prime, S_n tends to have large numbers of transitive subgroups, so this filter seems relatively coarse.

Second, if $P = h_1 \cdots h_r$ is a factorisation into irreducibles over $\mathbb{Z}$ where $2 \leq \deg(h_i) < \deg(P)$, G_i is the Galois group of h_i over $\mathbb{Q}$, and G is the Galois group of P over $\mathbb{Q}$, then $G \leq G_1 \times \cdots \times G_r$ is a subdirect product:

Definition 1.2.5. Let $G_1, \dots, G_r$ be finite groups, and G a subgroup of the direct product $G_1 \times \cdots \times G_r$. We say that G is a **subdirect product** of $G_1 \times \cdots \times G_r$ if the restricted projections $\pi_i : G \rightarrow G_i$ are all surjective.

The kernels of these projections gives an alternative definition: G is a subdirect product of $G_1 \times \cdots \times G_r$ if and only if there is a set of normal subgroups $\{N_1, \dots, N_r\}$ of G such that $G/N_i \cong G_i$ and $\bigcap_{i=1}^r N_i$ is trivial.

The fact that a Galois group of a reducible polynomial is a subdirect product is perhaps more intuitive in light of Goursat's Lemma, which relates subdirect products and fiber products in the case $r = 2$. A more general reference is:

Theorem 1.2.8. [42, Theorem 1.14 & subsequent corollaries] *Let*

$$P(x) = h_1(x) \cdots h_r(x)$$

be a factorisation into irreducibles over $\mathbb{Z}$. Let G be the Galois group of P over $\mathbb{Q}$, and G_i that of h_i . Then G is a subdirect product of $G_1 \times \cdots \times G_r$.

It is straightforward, although sometimes computationally expensive, to find all subdirect products of a given direct product. Since the number of such subgroups usually seems to be low, this provides a very fine filter on possible Galois groups. Table A.1 lists all subdirect products of all relevant direct products.

Finally and along these lines, it is straightforward to see that G cannot be equal to the direct product $G_1 \times \cdots \times G_r$. Indeed, by irreducibility of each h_i there would be an element $\sigma_i \in G_i$ that does not fix a root of h_i . But then the element $(\sigma_1, \dots, \sigma_r) \in G$ fixes no roots of P , contradicting the remark following Definition 1.2.4.

Therefore, G must be a proper subdirect product of $G_1 \times \cdots \times G_r$. This gives the following result, proved in Section 3.3:

Corollary 1.2.2. *Let $P(x) = h_1(x) \cdots h_r(x)$ be factored into irreducibles over $\mathbb{Z}$. If $|\text{Gal}(h_i(x)/\mathbb{Q})|$ are all coprime, then $P(x)$ is not intersective.*

1.3 Ergodic Theory

There is an alternative definition of intersective polynomials, coming from their namesake intersective sets in analytic number theory. The Furstenberg Correspondence Principle connects these sets to measure-preserving systems from ergodic theory. Since intersective polynomials have their historical origins from this subject, it is pertinent to describe these connections now. In place of formal proofs, we provide numerous references, both historical and contemporary.

Definition 1.3.1. Let $(X, \mathcal{A}, \mu)$ be a probability space (so that $\mu(X) = 1$). A measurable map $T : X \rightarrow X$ is called a **measure-preserving map** if, for all $A \in \mathcal{A}$, $\mu(T^{-1}(A)) = \mu(A)$. In this case, the tuple $(X, \mathcal{A}, \mu, T)$ is called a **measure-preserving system**.

Measure-preserving systems are foundational in ergodic theory, and are also the subject of the following celebrated theorem of Poincaré:

Theorem 1.3.1 (Poincaré Recurrence Theorem). *Let $(X, \mathcal{A}, \mu, T)$ be a measure-preserving system. For any $A \in \mathcal{A}$ with $\mu(A) > 0$, there exists $r \in \mathbb{Z}_{>0}$ such that*

$$\mu(A \cap T^{-r}(A)) > 0.$$

This theorem was stated by Poincaré (available in both the original French [56] and in an English historical review by Chenciner [14]) and rigorously proved by Carathéodory after developments in measure theory (again, the original German is available [13]; the proof is also standard in modern texts such as Barreira and Valls [6, Theorem 8.1]). It serves as a starting point in ergodic theory, and also has implications for thermodynamics and cosmology. It was strengthened in 1977 by Furstenberg [30]:

Theorem 1.3.2 (Furstenberg’s Multiple Recurrence Theorem). *Let $(X, \mathcal{A}, \mu, T)$ be a measure-preserving system. For any $k \in \mathbb{Z}_{>0}$ and any $A \in \mathcal{A}$ with $\mu(A) > 0$, there exists $r \in \mathbb{Z}_{>0}$ such that*

$$\mu(A \cap T^{-r}(A) \cap T^{-2r}(A) \cap \dots \cap T^{-(k-1)r}(A)) > 0.$$

These results motivate the following definition:

Definition 1.3.2. A set $R \subseteq \mathbb{Z}_{>0}$ is called a **set of recurrence** or a **recurrent set** if, for any measure-preserving system $(X, \mathcal{A}, \mu, T)$ and for all $A \in \mathcal{A}$ with $\mu(A) > 0$, there exists $r \in R$ such that $\mu(T \cap T^{-r}(A)) > 0$.

Thus Poincaré's theorem says that $\mathbb{Z}_{>0}$ itself is a set of recurrence. We give some more examples without proof:

Example 1.3.1. *The following are all sets of recurrence:*

1. *The set of values $\{f(n) \mid n \in \mathbb{Z}_{>0}\}$, where $f(x)$ is a polynomial with positive integer coefficients such that $f(0) = 0$ [31, Theorem 3.5].*
2. *The sets $\{p + 1 \mid p \text{ is prime}\}$ and $\{p - 1 \mid p \text{ is prime}\}$ [41, Example 3].*
3. *The set $\{\lfloor n^2 \alpha \rfloor \mid n \in \mathbb{Z}_{>0}\}$, where α is irrational [8, following Corollary 1.4].*

It turns out that sets of recurrence are connected to the rather more concrete notion of an intersective set.

Definition 1.3.3. Let $A \subseteq \mathbb{Z}$. The **upper density of A** is defined by

$$\bar{d}(A) := \limsup_{N \rightarrow \infty} \frac{|A \cap \{1, 2, \dots, N\}|}{N}.$$

Note that this limit, if it exists, is non-negative.

Definition 1.3.4. Let $I \subseteq \mathbb{Z}_{>0}$. We say that I is **intersective** if, for any set $A \subseteq \mathbb{Z}$ with positive upper density, we have $I \cap (A - A) \neq \emptyset$, where $A - A := \{a_1 - a_2 : a_1, a_2 \in A\}$ is the set of differences.

A celebrated theorem proved independently by Furstenberg [30, Theorem 1.2] and Sárközy [64, the first theorem] provides an example of an intersective set:

Theorem 1.3.3 (Furstenberg-Sárközy Theorem). *If $A \subseteq \mathbb{Z}$ has positive upper density, then A contains two distinct elements whose difference is a perfect square. In other words, the set of positive squares in $\mathbb{Z}$ is intersective.*

This theorem has a rich history with numerous different proofs by Furstenberg, Sárközy, Kamae-Mendès France, Green [35, Theorem 2, Section 3], Lyall [45, Theorem 2], and Green-Tao-Ziegler [36]; proof methods have included ergodic theory, the circle method of analytic

number theory, the theory of van der Corput sets, and perhaps the most elementary method which relies principally on the Cauchy-Schwarz inequality.

The following, proved by Furstenberg [30, Section 1], connects sets of recurrence and intersective sets, thereby connecting ergodic theory with analytic number theory:

Theorem 1.3.4 (Furstenberg Correspondence Principle). *Let $E \subseteq \mathbb{Z}_{>0}$. Then there exists a measure-preserving system $(X, \mathcal{A}, \mu, T)$ and a set $A \in \mathcal{A}$ with $\mu(A) = \bar{d}(E)$ such that, for any $r_1, \dots, r_k \in \mathbb{Z}_{>0}$,*

$$\mu(A \cap T^{-r_1}(A) \cap \dots \cap T^{-r_k}(A)) \leq \bar{d}(E \cap (E - r_1) \cap \dots \cap (E - r_k)).$$

In particular, this shows that sets of recurrence are also intersective. In fact, the converse is also true, c.f., Furstenberg, Katznelson, and Ornstein [32, pp. 528–529] or Moreira [51, Theorem 10]:

Theorem 1.3.5. *Let $I \subseteq \mathbb{Z}_{>0}$ be intersective. Then I is also a set of recurrence.*

We now give an alternative to our main definition, Definition 1.1.1, and we subsequently explain why the two notions are consistent:

Definition 1.3.5. We say that $P(x) \in \mathbb{Z}[x]$ is **intersective** if the set of positive values $\{P(n) \mid n \in \mathbb{Z}\} \cap \mathbb{Z}_{>0}$ is intersective.

Kamae and Mendès France, in their work proving the Furstenberg-Sárközy Theorem [41], gave the following sufficient conditions for intersectivity:

Theorem 1.3.6 (Kamae-Mendès France). *A set $H \subseteq \mathbb{Z}_{>0}$ is intersective if, for every integer $m \neq 0$, the set $H_m = \{h \in H : m \mid h\}$ is infinite, and the sequence αH_m is uniformly distributed modulo 1 for every irrational α .*

This offers a second explanation why, for example, the sets of positive squares and the primes ± 1 are intersective. Finally, the connection to the previous section has now become clear:

Corollary 1.3.1. *A polynomial $P(x) \in \mathbb{Z}[x]$ is intersective if and only if P has a root modulo m for every positive integer m .*

Therefore, intersective polynomials provide examples of intersective sets for ergodic theorists and analytic number theorists. We will not return to this perspective, but it places the results of this thesis in a wider historical and mathematical context.

1.4 A Word on Function Fields

One of the strengths of our approach to proving Theorem 1.1.3 is the independence on the arithmetic of the ground field, relying instead on pure Galois theory. This means that our results translate in a straightforward way to polynomials over function fields.

Recall that a **global field** is either a number field or a **function field**, i.e., a finite separable extension of a field of rational functions $\mathbb{F}_q(T)$, where q is a prime power.

There are many fruitful analogies between number fields and function fields. With this in mind, Mishra [50] proved an analogue of Theorem 1.2.2 for arbitrary global fields.

Let $\mathcal{O}_K$ denote the usual ring of integers of K when K is a number field, or the integral closure of $\mathbb{F}_q[T]$ when K is a function field.

Definition 1.4.1. A polynomial in $P(x) \in \mathcal{O}_K[x]$ is called **intersective** if for every subgroup $\Gamma \leq \mathcal{O}_K$ of finite index, there exists $\lambda \in \mathcal{O}_K$ such that $P(\lambda) \equiv 0 \pmod{\Gamma}$, i.e., $P(\lambda) \in \Gamma$. We call an intersective polynomial $P(x) \in \mathcal{O}_K[x]$ **strongly intersective** if P does not have a root in K .

Let $P(x) \in \mathcal{O}_K[x]$ such that no non-unit divides every coefficient of P . Factor P into irreducibles over K as $P(x) = h_1(x) \cdots h_r(x)$; if K is a function field, also assume that each h_i is separable.

The algebraic setup is as follows: Let L be a splitting field of P over K , $G = \text{Gal}(L/K)$, θ_i a fixed root of h_i , $K_i = K(\theta_i)$, and $H_i = \text{Aut}(L/K_i) \leq G$. Let $U = \bigcup_{i=1}^r H_i \subseteq G$.

Now for the arithmetic setup: Let

- $\mathfrak{q}_i$ be the discriminant ideal of h_i , which is non-zero by separability;
- $\mathfrak{r}_i = \text{Res}(h_i, h'_i)$;
- $\mathfrak{q} = \mathfrak{r}_1 \cdots \mathfrak{r}_r = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_s^{b_s}$, the prime factorisation of $\mathfrak{q}$ in the Dedekind domain $\mathcal{O}_K$;
- $\Delta := \mathfrak{p}_1^{2b_1+1} \cdots \mathfrak{p}_s^{2b_s+1}$;
- if K is a number field, define

$$D := \prod_{i=1}^r (\mathfrak{q}_i)^{(n_1! \cdots n_r!) \left(1 - \frac{1}{n_i}\right)};$$

- if K is a function field, define

$$\Delta' = \sum_{i=1}^v b_i \deg(\mathfrak{p}_i) \in \mathbb{Z},$$

$$D' = \prod_{i=1}^r n_i!,$$

and

$$d = [K : \mathbb{F}_q(T)].$$

We have the following generalisation of Theorem 1.2.2 due to Mishra:

Theorem 1.4.1. [50, Theorem 1] *The following are equivalent:*

1. $P(x)$ is intersective.
2. $P(x) \equiv 0 \pmod{\Delta}$ is solvable in $\mathcal{O}_K$, and

$$\bigcup_{\sigma \in G} \sigma^{-1} U \sigma = G.$$

In particular, the conjugate-covering condition on the Galois group G of P is necessary for intersectivity over all global fields.

In fact, the other algebraic constraints on G are valid over function fields as well. Therefore, it is feasible to use our methods to find examples of strongly intersective polynomials over both function fields and finite extensions of number fields.

Chapter 2

Local Structure of Intersective Polynomials

In this Chapter, we prove some results on intersective polynomials, focusing on ramified primes. Section 2.1 demonstrates that intersectivity can be viewed as a field-theoretic property, which helps make sense of the preceding sentence. Section 2.2 extends Theorem 1.1.1 in a way that justifies its inclusion in this section. In both Sections, we provide implementations in SageMath which can be found on the author's GitHub [5].

2.1 p -Adic Roots

In this section, we will prove that intersectivity of a polynomial is really a condition on its splitting field over $\mathbb{Q}$ together with its set of intermediate fields corresponding to its irreducible factors. We begin by recalling a standard result on finite extensions of $\mathbb{Q}_p$ from Section D.6:

Theorem D.6.3. *Let $L/\mathbb{Q}$ be a number field; say $L = \mathbb{Q}(\theta)$, where θ has minimal polynomial $f(x) \in \mathbb{Q}[x]$. Then the inequivalent extensions of the p -adic absolute value $|\cdot|_p$ to L are in bijection with the irreducible factors of $f(x)$ in $\mathbb{Q}_p[x]$. In particular, there are finitely many such extensions.*

Proof. Let $f(x) = g_1(x) \cdots g_r(x) \in \mathbb{Q}_p[x]$ be the factorisation of f into irreducibles, and let $\widehat{L}_i := \mathbb{Q}_p[x]/\langle g_i(x) \rangle$, which is a p -adic field of degree $\deg(g_i)$. In particular, $\widehat{L}_i$ is complete

by Proposition D.6.1. By Theorem D.6.2, $|\cdot|_p$ on $\mathbb{Q}_p$ extends uniquely to $\widehat{L}_i$; call this unique extension $|\cdot|_i$.

By Lemmas D.6.2 and D.6.3, we have a composition of maps

$$\tau : L \hookrightarrow L \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{i=1}^r \widehat{L}_i \rightarrow \widehat{L}_i.$$

Thus, we can define $|\cdot|_L$ on L by pulling back $|\cdot|_i$. In other words, for $\alpha \in L$, let

$$|\alpha|_L := |\tau(\alpha)|_i.$$

Thus, for each i we obtain a discrete absolute value $|\cdot|_L$ on L extending $|\cdot|_p$.

Conversely, suppose $|\cdot|$ is a discrete absolute value on L extending $|\cdot|_p$. Let $\widehat{L}$ denote its completion, which comes with an embedding $\iota : L \hookrightarrow \widehat{L}$. Note that $\mathbb{Q}_p(\iota(\theta))$ is complete and contains $\iota(L)$ as a dense subset, so by uniqueness of completions, we have $\widehat{L} = \mathbb{Q}_p(\iota(\theta))$. If $g(x) \in \mathbb{Q}_p[x]$ is the minimal polynomial of $\iota(\theta)$, then $f(\iota(\theta)) = 0$, so $g(x) = g_i(x)$ for some i . This forces $\widehat{L} = \widehat{L}_i$, finishing the proof. $\square$

Now every discrete absolute value on a number field arises from a prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ (Proposition D.6.1). Thus, concerning the case where one of the $g_i(x)$ is linear, we have the following consequence:

Corollary 2.1.1. *Let $f(x) \in \mathbb{Q}[x]$ be irreducible, $p \in \mathbb{Z}$ be a prime, and $\mathbb{Q}(\theta)/\mathbb{Q}$ a number field. Then θ embeds as a root of f into $\mathbb{Q}_p$ if and only if there is a prime $\mathfrak{p}$ of L above p such that the completion $\widehat{L}$ of L at $\mathfrak{p}$ is isomorphic to $\mathbb{Q}_p$.*

Applying this result factor-by-factor to a reducible polynomial gives our first contribution, Corollary 1.1.1:

Corollary 1.1.1. *Let $P(x) = h_1(x) \cdots h_r(x) \in \mathbb{Z}[x]$ be factored into irreducibles. Then P is intersective if and only if, for each rational prime p , there is an i , a root θ_i of h_i , and a prime $\mathfrak{p}_i$ of $\mathbb{Q}(\theta_i)$ above p such that the completion of $\mathbb{Q}(\theta_i)$ at $\mathfrak{p}_i$ is isomorphic to $\mathbb{Q}_p$.*

In particular, for two such polynomials $P = h_1 \cdots h_r$ and $P' = h'_1 \cdots h'_r$ with $\deg(h_i) = \deg(h'_i)$, if each element of the set $\{\mathbb{Q}[x]/\langle h_i(x) \rangle\}$ is isomorphic to an element of $\{\mathbb{Q}[x]/\langle h'_j(x) \rangle\}$ and vice versa, then the intersectivity of P and P' is equivalent.

We obtain our other Corollary 1.1.2 using the following standard result from Section D.5:

Theorem D.5.1. Let $\widehat{L}/\mathbb{Q}$ be a p -adic field of degree n with ramification degree $e_{\widehat{L}}$ and inertia degree $f_{\widehat{L}}$. Then $n = e_{\widehat{L}}f_{\widehat{L}}$.

Proof. Let $\pi_{\widehat{L}}$ be a uniformiser of $\widehat{L}$. By definition, $p\mathcal{O}_{\widehat{L}} = \langle \pi_{\widehat{L}} \rangle^{e_{\widehat{L}}}$, so we have the filtration

$$\mathcal{O}_{\widehat{L}} \supseteq \langle \pi_{\widehat{L}} \rangle \supseteq \langle \pi_{\widehat{L}} \rangle^2 \supseteq \cdots \supseteq \langle \pi_{\widehat{L}} \rangle^{e_{\widehat{L}}-1} \supseteq \langle \pi_{\widehat{L}} \rangle^{e_{\widehat{L}}} = p\mathcal{O}_{\widehat{L}}, \quad (2.1)$$

and the successive quotients are

$$\langle \pi_{\widehat{L}} \rangle^j / \langle \pi_{\widehat{L}} \rangle^{j+1}, \quad 0 \leq j \leq e_{\widehat{L}} - 1.$$

For each j , the multiplication-by- $\pi_{\widehat{L}}^j$ map induces an isomorphism of $\mathcal{O}_{\widehat{L}}/\langle \pi_{\widehat{L}} \rangle$ -modules

$$\mathcal{O}_{\widehat{L}}/\langle \pi_{\widehat{L}} \rangle \rightarrow \langle \pi_{\widehat{L}} \rangle^j / \langle \pi_{\widehat{L}} \rangle^{j+1},$$

so each $\langle \pi_{\widehat{L}} \rangle^j / \langle \pi_{\widehat{L}} \rangle^{j+1}$ is isomorphic as an $\mathbb{F}_p$ -vector space to the residue field $\mathcal{O}_{\widehat{L}}/\langle \pi_{\widehat{L}} \rangle = \kappa_{\widehat{L}}$. By definition, $\kappa_{\widehat{L}}$ has dimension $f_{\widehat{L}}$ over $\mathbb{F}_p$.

Now we use the filtration (1.2) to build a direct sum decomposition of $\mathcal{O}_{\widehat{L}}/p\mathcal{O}_{\widehat{L}} = \mathcal{O}_{\widehat{L}}/\langle \pi_{\widehat{L}} \rangle^{e_{\widehat{L}}}$. Indeed, the map

$$\mathcal{O}_{\widehat{L}}/p\mathcal{O}_{\widehat{L}} \rightarrow \bigoplus_{j=0}^{e_{\widehat{L}}-1} \langle \pi_{\widehat{L}} \rangle^j / \langle \pi_{\widehat{L}} \rangle^{j+1},$$

$$\alpha + p\mathcal{O}_{\widehat{L}} \mapsto (\alpha + \langle \pi_{\widehat{L}} \rangle, \alpha + \langle \pi_{\widehat{L}} \rangle^2, \dots, \alpha + \langle \pi_{\widehat{L}} \rangle^{e_{\widehat{L}}})$$

can be shown to be an isomorphism of $\mathbb{F}_p$ -vector spaces (surjectivity is the trickiest part, but one can build a lift of a residue class inductively on j). Thus $\mathcal{O}_{\widehat{L}}/p\mathcal{O}_{\widehat{L}}$ has dimension $e_{\widehat{L}}f_{\widehat{L}}$ as an $\mathbb{F}_p$ -vector space.

Let $b_1, \dots, b_f \in \mathcal{O}_{\widehat{L}}$ be elements whose residue classes $\overline{\mathcal{B}} := \{b_1 + \langle \pi_{\widehat{L}} \rangle, \dots, b_f + \langle \pi_{\widehat{L}} \rangle\}$ in $\mathcal{O}_{\widehat{L}}/\langle \pi_{\widehat{L}} \rangle$ form an $\mathbb{F}_p$ -basis. For each j , $0 \leq j \leq e_{\widehat{L}} - 1$, $\{b_1\pi_{\widehat{L}}^j, \dots, b_f\pi_{\widehat{L}}^j\}$ descends to an $\mathbb{F}_p$ -basis of $\langle \pi_{\widehat{L}} \rangle^j / \langle \pi_{\widehat{L}} \rangle^{j+1}$ via the multiplication-by- $\pi_{\widehat{L}}^j$ map. Collecting over all such j shows that $\{b_i\pi_{\widehat{L}}^j + \langle \pi_{\widehat{L}} \rangle^{j+1} : 1 \leq i \leq f, 0 \leq j \leq e_{\widehat{L}} - 1\}$ is an $\mathbb{F}_p$ -basis of $\mathcal{O}_{\widehat{L}}/p\mathcal{O}_{\widehat{L}}$.

Finally, by Nakayama's Lemma D.5.1, $\{b_i\pi_{\widehat{L}}^j : i \leq 1 \leq f_{\widehat{L}}, 0 \leq j \leq e_{\widehat{L}} - 1\}$ is a minimal

generating set of $\mathcal{O}_{\hat{L}}$ as a $\mathbb{Z}_p$ -module, and since $\mathcal{O}_{\hat{L}}$ is free as a $\mathbb{Z}_p$ -module, this minimal generating set is a $\mathbb{Z}_p$ -basis for $\mathcal{O}_{\hat{L}}$. As $\mathcal{O}_{\hat{L}}$ has rank n over $\mathbb{Z}_p$, this finishes the proof. $\square$

Corollary 1.1.2. *Let $f \in \mathbb{Q}[x]$ be irreducible of degree ≥ 2 with root θ , Galois group G over $\mathbb{Q}$, and $n = [L : \mathbb{Q}] = |G| \geq 2$. Let p be a rational prime which ramifies in $\mathbb{Q}(\theta)$, and $\mathfrak{p}$ a prime of $\mathbb{Q}(\theta)$ above p . Then θ embeds into $\mathbb{Q}_p$ as a root of f via the embedding defined by $\mathfrak{p}$ if and only if the ramification and inertia degrees $e(\mathfrak{p}/p)$ and $f(\mathfrak{p}/p)$ of $\mathfrak{p}$ over p are both 1.*

More generally, let $P(x) = h_1(x) \cdots h_r(x) \in \mathbb{Q}[x]$ be factored into irreducibles, and let p be a rational prime which is ramified in a splitting field of P over $\mathbb{Q}$. Then P has a root in $\mathbb{Q}_p$ if and only if, for some $1 \leq i \leq r$, there is a root θ_i of h_i such that one of the primes of $\mathbb{Q}(\theta_i)$ above p has ramification and inertia degrees equal to 1.

Of course, this result holds for both unramified and ramified primes, but it is only algorithmic for the latter, finite family of primes, while the methods of Chapters 3 and 4 seem more efficient for unramified primes.

Along these lines, this furnishes an algorithm for checking intersectivity at ramified primes, which was implemented in SageMath, c.f.,

“check_intersectivity_ramification_degrees.sage”

on the author’s GitHub [5]. A direction for future work is to use this (or the algorithm in the next section), together with the later, Galois-theoretic algorithm for unramified primes, to find all strongly intersective polynomials with coefficients within certain bounds.

2.2 Decomposition Groups

In this section, we will extend a theorem of Jack Sonn, which in turn is a variant of Theorem 1.2.2 in terms of decomposition groups.

Theorem 1.1.1. [61, Proposition 1] *Let $L/\mathbb{Q}$ be a finite Galois extension with Galois group G . The following are equivalent:*

1. *L is the splitting field of a product $P = h_1 \cdots h_r$ of irreducible polynomials of degree greater than 1 in $\mathbb{Q}[x]$, and P has a root in $\mathbb{Q}_p$ for all primes p .*

2. G is the union of the conjugates of r proper subgroups $H_1, \dots, H_r$, the intersection of all these conjugates is trivial, and for all primes $\mathfrak{p}$ of L , the decomposition group $D_L(\mathfrak{p} \mid p)$ is contained in a conjugate of some H_i .

Using ideas from the proof of Theorem 1.2.2, we prove the generalisation, Theorem 1.1.2:

Theorem 1.1.2. *Let $L/\mathbb{Q}$ be a finite Galois extension with Galois group G . The following are equivalent:*

- (1) L is the splitting field of a product $P = h_1 \cdots h_r$ of irreducible polynomials of degree greater than 1 in $\mathbb{Q}[x]$, and P has a root in $\mathbb{Q}_p$ for all primes p .
- (2) G is the union of the conjugates of r proper subgroups $H_1, \dots, H_r$, the intersection of all these conjugates is trivial, and for all primes $\mathfrak{p}$ of L lying over a ramified prime $p \in \mathbb{Z}$, the decomposition group $D_L(\mathfrak{p} \mid p)$ is contained in a conjugate of some H_i .

Proof. The only change from Sonn's proof is to prove that (2) always implies (1) for unramified primes. To this end, let $p \in \mathbb{Z}$ be a prime which is unramified in L . Let $U = \bigcup_{i=1}^r H_i \subseteq G$, so the first assumption in (2) can be written as

$$G = \bigcup_{\sigma \in G} \sigma^{-1} U \sigma. \quad (2.2)$$

Since p is unramified, we have the factorisation

$$p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_g,$$

where each $\mathfrak{p}_i$ is a distinct prime of L . We also have the set of Frobenius elements of p in L (see Section D.3):

$$\text{Frob}_L(p) = \{\text{Frob}_L(\mathfrak{p}_1 \mid p), \dots, \text{Frob}_L(\mathfrak{p}_g \mid p)\}.$$

Let $\theta_1, \dots, \theta_r \in L$ be such that $H_i = \text{Aut}(L/\mathbb{Q}(\theta_i))$, and let $h_i(x) \in \mathbb{Q}[x]$ be the minimal polynomial of θ_i . Then we define $P(x) := h_1(x) \cdots h_r(x)$. Now by definition of P and the H_i , P having a root in $\mathbb{Q}_p$ is equivalent to $\text{Frob}_L(\mathfrak{p}_i \mid p) \in H_j$ for some i and j [7, Lemma 2]. By equation (2.2), we know that for any $1 \leq \ell \leq g$ there is some $1 \leq j \leq r$

and some $\sigma \in G$ such that $\text{Frob}_L(\mathfrak{p}_\ell \mid p) \in \sigma^{-1}H_j\sigma$, so $\sigma \text{Frob}_L(\mathfrak{p}_\ell \mid p)\sigma^{-1} \in H_j$. But $\sigma \text{Frob}_L(\mathfrak{p}_\ell \mid p)\sigma^{-1}$, being a conjugate of a Frobenius element, is also a Frobenius element (see Proposition D.3.3), i.e., there is some $1 \leq i \leq g$ such that

$$\sigma \text{Frob}_L(\mathfrak{p}_\ell \mid p)\sigma^{-1} = \text{Frob}_L(\mathfrak{p}_i \mid p) \in H_j.$$

Thus P has a root in $\mathbb{Q}_p$. □

Theorem 1.1.2 constitutes yet another algorithm for checking intersectivity at ramified primes by checking conditions on finitely many decomposition groups, and a SageMath implementation of this algorithm can be found on the author's GitHub [5], file name “check_intersectivity_decomposition_groups.sage”.

Chapter 3

The Galois Theory of Intersective Polynomials

In this Chapter, we will discuss the main algebraic tools used to check intersectivity. Section 3.1 describes the possible transitive degrees of the Galois group of a reducible polynomial. Section 3.2 discusses conjugate covering of finite groups; the algorithm contained therein, implemented in GAP, comprises the bulk of the computational work in this thesis. Section 3.3 concerns proper subdirect products of direct products of Galois groups. All such subgroups up to degree 10 (with the largest degree of an irreducible factor being 8) were found computationally via SageMath. As usual, the algorithms can be found on the author's GitHub [5].

It is the author's hope that the data contained in this Chapter can be used to support or generate new conjectures of this type, especially as subgroup databases are extended to accommodate more factorisations. We give some examples of observations and conjectures in Section 4.2.

3.1 Transitivity Degrees

Suppose $P(x) = h_1(x) \cdots h_r(x)$, where the h_i are distinct and irreducible over $\mathbb{Z}$. A splitting field L of the reducible polynomial $P = h_1 \cdots h_r$ can be constructed as a compositum $L_1 \cdots L_r$ of splitting fields of the h_i ; in particular, if $d_i = \deg(h_i)$, then its degree is a multiple of $\text{lcm}(d_1, \dots, d_r)$ and a divisor of $\prod_{i=1}^r d_i$. Thus, the Galois group G of $L/\mathbb{Q}$ is a transitive subgroup of S_n for some n with these arithmetic properties. On the other

hand, G is a subgroup of $G_1 \times \cdots \times G_r$ for $G_i := \text{Gal}(h_i/\mathbb{Q})$ (see Section 3.3), hence also a subgroup of $S_{d_1} \times \cdots \times S_{d_r}$.

Thus, given sufficient transitive subgroup data and full subgroup data for various direct products of symmetric groups, one can produce a finite list of possible Galois groups of strongly intersective polynomials of bounded degree. The [L-functions and modular forms database \(LMFDB\)](#) [44] is a suitable database.

The [Abstract Group](#) section of LMFDB contains complete subgroup data for the relevant groups. In fact, this part of LMFDB would be sufficient for polynomials of degree 11 as well, but degree 11 brings transitive degrees as high as 54, and transitive subgroups of S_{54} have not yet been classified.

The [Galois Group](#) section of LMFDB allows searching by transitive degree, and is complete up to and including degree 47, with the exception of degree 32 - there are almost 3 million such groups. This demonstrates the observation in finite group theory that finite p -groups, i.e., groups whose order is a power of a prime p , are by far the most numerous, and since powers of 2 are more dense than other prime powers, 2-groups seem to completely dominate the number of groups up to a given order. See Besche, Eick, and O’Brien [9, Table 1] for a quantitative observation of this phenomenon.

Therefore, some care is required to ensure that we do not miss any groups in degree 32. Transitive groups of degree 32 come up in this thesis for three possible factorisations of degree-10 polynomials, namely $(2, 2, 2, 2, 2)$, $(2, 2, 2, 4)$, and $(2, 4, 4)$. The LMFDB interface is simpler for our purposes, so we prefer it when it is complete - fortunately, the LMFDB data are actually complete in degree 32 up to subgroups of order 511 (inclusive), and only $C_2 \times S_4$ has proper subgroups larger than this, namely three subgroups of order 576. Thus, we can check these three subgroups with [GAP’s transitive group package](#), which includes degree 32 as a separate package due to its unwieldy size.

The author wrote a Python script to query LMFDB’s API and find all subgroups of direct products of symmetric groups which also embed transitively in the appropriate degrees. This is available in the file named “search_possible_galois_groups.py” on the author’s GitHub [5]. The output is a list of LMFDB abstract group labels (which agree with the GAP small group labels when they are present). We treat this as a first filter on possible Galois groups, then check which of them can be conjugate-covered by subgroups of the relevant indices, as described in the following Section 3.2. In hindsight, if the author had noticed the comparatively low number of groups appearing in the following two sections, then it would have been far more efficient to use this method as a final filter.

3.2 Conjugate Covering

Equipped with a finite list of groups that surely encompasses all possible strongly inter-sective Galois groups, we proceed to our next algebraic filter, namely Condition 1.1.

Recall the following definition from Section 1.2:

Definition 1.2.1. Let G be a finite group with subgroups $H_1, \dots, H_r$. We say that G is **conjugate-covered by the H_i** if

$$G = \bigcup_{\sigma \in G} \bigcup_{i=1}^r \sigma^{-1} H_i \sigma.$$

The author wrote a GAP function to check whether a given finite group G can be conjugate-covered by r subgroups with indices $n_1, \dots, n_r$; note that, in our context, the tuple $(n_1, \dots, n_r)$ is exactly a factorisation type of a reducible polynomial of degree $n_1 + \dots + n_r$, with n_i being the degree of the i^{th} irreducible factor.

Any groups that can be covered in such a way, which are also transitive subgroups of appropriate degree as described in the previous Section 3.1, appear in Table B.1.

The GAP function is available on the author’s GitHub [5], file name “CheckConjugate-Covering.g”; it produces a .txt file with comprehensive data on possible subgroup choices, i.e., possible choices of $H_i = \text{Aut}(L/\mathbb{Q}(\theta_i))$, and the union sizes of their conjugates, effectively giving the number of derangements of G with respect to its action on the roots θ_i . This thesis is primarily concerned with whether this number is 0, as this would indicate a possible Galois group of a strongly inter-sective polynomial, but the full data will doubtless be useful for future analysis.

Analysing Table B.1, we see that a factorisation into two irreducibles of the same degree never works. This supports Conjecture 2 in a recent pre-print of Ellis and Harper [25]; note that they proved the special case when one of the corresponding subgroups defined by a single root is maximal. This table provides evidence for the full conjecture, i.e., without the maximality assumption; for example, in the degree-8 factorisation $8 = 4 + 4$, the dihedral group D_4 of order 8 is a subgroup of S_4^2 which is also transitive in S_4 , and is not conjugate-covered by any pair of subgroups of index 4, despite none of these subgroups being maximal. Altogether, there are 14 subgroups that give examples of this type, with the largest order being 64. In the other two factorisations considered in this thesis which

could possibly provide additional examples, namely $6 = 3 + 3$ and $10 = 5 + 5$, all of the relevant subgroups are maximal. Of course, these latter examples do not disprove the conjecture - they merely confirm the already-proved Corollary 4 from the same paper.

Theorem 3 from this paper states that a finite group cannot be conjugate-covered by proper subgroups H_1 and H_2 if $|H_2|$ divides $|H_1|$, provided that H_2 is maximal. There is no clear way to remove the maximality assumption, but several examples from this thesis suggest that the result would still hold. For example, in the factorisation $6 = 2 + 4$, none of the subgroups of $C_2 \times C_4$ of index 4 are maximal, yet it is not conjugate-covered by a subgroup of index 2 and one of index 4. This factorisation gives a total of 4 examples of this nature, with the largest having order 16. Similarly, in the factorisation $8 = 2 + 6$, we have 17 examples supporting this extended theorem, with the largest having order 144; the factorisation $9 = 3 + 6$ gives 39 examples, up to order 432; and finally, the factorisation $10 = 2 + 8$ gives 82 examples, up to order 2304.

3.3 Subdirect Products

Finally, we introduce our last algebraic filter, which will produce the table of possible Galois groups of strongly intersective polynomials. We recall the relevant definition and result from Section 1.2:

Definition 1.2.5. Let $G_1, \dots, G_r$ be finite groups, and G a subgroup of the direct product $G_1 \times \dots \times G_r$. We say that G is a **subdirect product** of $G_1 \times \dots \times G_r$ if the restricted projections $\pi_i : G \rightarrow G_i$ are all surjective.

From the kernels of these projections we can construct an alternative, intrinsic definition: G is a subdirect product of $G_1 \times \dots \times G_r$ if and only if there is a set of normal subgroups $\{N_1, \dots, N_r\}$ of G such that $G/N_i \cong G_i$ and $\bigcap_{i=1}^r N_i$ is trivial.

Theorem 1.2.8. [42, Theorem 1.14 & subsequence corollaries] *Let*

$$P(x) = h_1(x) \cdots h_r(x)$$

be a factorisation into irreducibles over $\mathbb{Z}$. Let G be the Galois group of P over $\mathbb{Q}$, and G_i that of h_i . Then G is a subdirect product of $G_1 \times \dots \times G_r$.

In fact, we can refine this further in the case of intersective polynomials:

Corollary 3.3.1. *Let $P(x) = h_1(x) \cdots h_r(x)$ be a factorisation into irreducibles over $\mathbb{Z}$. Let G be the Galois group of P over $\mathbb{Q}$, and G_i that of h_i . If P is intersective, then G is a **proper** subdirect product of $G_1 \times \cdots \times G_r$.*

Proof. Otherwise, by irreducibility of the h_i there would be an element $\sigma_i \in G_i$ that does not fix a root of h_i . Note that the element $(\sigma_1, \dots, \sigma_r) \in G_1 \times \cdots \times G_r = G$ would then fix no root of P . However, this contradicts the remark following Definition 1.2.4. $\square$

Combined with the requirement that $|G|$ is divisible by $|G_i|$ (by virtue of the existence of the quotient $G/N_i \cong G_i$), we see that $|G|$ is divisible by $\text{lcm}(|G_1|, \dots, |G_r|)$, and we have proved our Corollary 1.2.2:

Corollary 1.2.2. *Let $P(x) = h_1(x) \cdots h_r(x)$ be factored into irreducibles over $\mathbb{Z}$. If $|\text{Gal}(h_i(x)/\mathbb{Q})|$ are all coprime, then $P(x)$ is not intersective.*

One can make other observations about the (non-)existence of proper subdirect products. For example, if $G_1 \times \cdots \times G_r$ contains many simple subgroups, then one expects comparatively few subdirect products. In particular, the G_i themselves are natural candidates for subdirect products (if their orders are large enough), so the G_i being simple will result in few subdirect products.

Either definition for subdirect product can be used to exhaustively find all subdirect products of a given direct product. This is the SageMath algorithm, file name “find_subdirect_products.sage”, on the author’s GitHub [5]. Using this produces Table A.1 in Appendix A.

Chapter 4

Possible Galois Groups of Strongly Intersective Polynomials

In this Chapter, we reap the benefits of building the tables from Chapter 3. In Section 4.1, we explain the proof of our classification result, Theorem 1.1.3, and illustrate the process of using Table C.1 to find specific strongly intersective polynomials with desired Galois group. We also discuss some immediate observations that can be made. In Section 4.2, we comment on minimal intersectivity and state some novel conjectures generated from Table C.1.

4.1 The Classification Theorem

We are now ready to prove Theorem 1.1.3:

Theorem 1.1.3. *Let P be a strongly intersective polynomial with Galois group G over $\mathbb{Q}$. If $5 \leq \deg(P) \leq 10$, then G must be one of the groups appearing in Table C.1.*

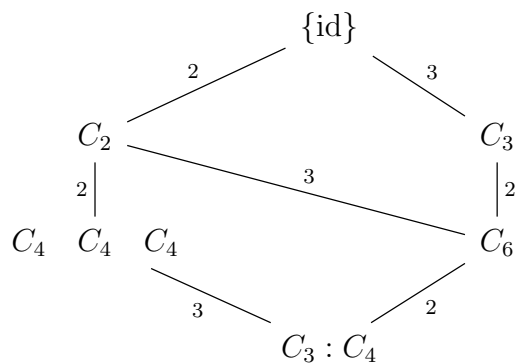
Proof. Starting with Table A.1 of subdirect products, which surely encompasses all such Galois groups, we then check which groups also appear in Table B.1. Finally, we check which of the remaining groups can be embedded in (products of) symmetric groups as described in Section 3.1. $\square$

Examples are given for each group arising from polynomials up to degree 8, with some examples given in degree 9, and fewer for degree 10; a reasonable goal for future research

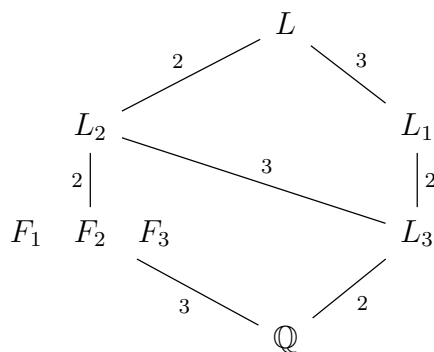
is to fill these gaps. Note that these gaps are present mostly due to external constraints like computational difficulty. In particular, there is no evidence that those groups with no examples cannot be realised through a strongly intersective polynomial. In other words, if a reducible polynomial has “intersective behaviour” at its unramified primes, then Table C.1 provides evidence that the polynomial’s coefficients can always be adjusted to achieve “intersective behaviour” at its ramified primes too.

We now illustrate the process of finding examples.

Consider the factorisation $9 = 2 + 3 + 4$ and the Galois group $C_3 : C_4$ (12.1). As always, write $P(x) = h_1(x)h_2(x)h_3(x)$ where P has degree 9, h_1 has degree 4, h_2 has degree 3, and h_3 has degree 2. Table A.1 indicates that $G := \text{Gal}(P/\mathbb{Q}) = C_3 : C_4$ can only occur when h_1 is a C_4 -quartic and h_2 is an S_3 -cubic. Let $L/\mathbb{Q}$ be a splitting field of P , $L_i/\mathbb{Q}$ that of h_i , and $d_i = \text{disc}(h_i)$. Then L_1 has a unique quadratic subfield given by $\mathbb{Q}(\sqrt{d_1})$, and similarly for L_2 and d_2 . In fact, analysing the subgroup lattice for $C_3 : C_4$ given below (flipped vertically; available at [LMFDB’s Abstract Group database](#)),



gives the field diagram



where the F_i form a conjugacy class of cubic subfields of L_2 . More importantly, the diagram shows that there is only one quadratic subfield of L ; hence L_1 and L_2 must have the same unique quadratic subfield, which must also be L_3 itself. In other words, the square-free parts of the polynomial discriminants d_1 , d_2 , and d_3 are all equal. It is straightforward to use [LMFDB's Number Fields database](#) to find such triplets of fields and their defining polynomials, for example $x^4 - x^3 + x^2 - x + 1$, $x^3 - 12x - 4$, and $x^2 - x - 1$, whose product will have the desired Galois group.

Of course, the above does not distinguish between arithmetic properties of different ramified primes, which must be controlled in order to guarantee intersectivity. The author has not found a better general method than trial-and-error using Corollary 1.1.2; such an improved method represents an important direction for future work.

At the same time, one's expectations must be tempered if searching for such general results: A central theorem of Class Field Theory states that splitting patterns of primes in number fields can be described by congruence conditions precisely when the field is Abelian. This seems to be originally due to Teiji Takagi, with a historical account being given by Conrad [20, Section 5, specifically Theorems 5.11 and 5.12]. Alternatively, the first of Olga Taussky-Todd's appendices to Harvey Cohn's Class Field Theory text [16] consists of notes from a celebrated lecture series by Emil Artin in Göttingen, 1932, which greatly simplified the existing work on the subject.

A consequence of the above is that it is unclear what form one might expect to be taken by general intersectivity conditions on polynomial coefficients. For the above reasons, in the Abelian case one expects conditions analogous to Theorem 1.2.7, although potentially much more complicated. In non-Abelian settings, there are examples where prime splitting patterns are encapsulated in the coefficients of a certain modular form [27].

4.2 Observations and Conjectures

There are several observations that one can make from Table C.1, and some Galois groups that might correspond to obvious factorisations for a given degree are absent from said Table, leading to some novel conjectures on factorisations and Galois groups of strongly intersective polynomials.

First, we prove a consequence of Theorem 1.1.3 which is not group-theoretically sophisticated, but may have been elusive without the overview provided by Table C.1.

In degree 5, we have the possible Galois group of a strongly intersective polynomial S_3 arising from the factorisation shape $(2, 3)$ as a product of a quadratic and an S_3 -cubic with

overlapping splitting fields. From Table A, we see that S_{n-2} is always a subdirect product of $C_2 \times S_{n-2}$, so at first glance, one might expect this pattern to continue. However, for $n > 5$, S_{n-2} does not appear in Table B.1 for the factorisation shape $(2, n-2)$, implying in particular that it is never the Galois group of a strongly intersective polynomial with such a factorisation.

For odd degrees, this can be explained with the following standard result:

Lemma 4.2.1. *Let $m \geq 5$. Then all subgroups of the symmetric group S_m with index m are conjugates of each other and isomorphic to S_{m-1} . In particular, all subgroups of S_m of index $m-1$ consist of permutations with exactly one fixed point.*

Proof. Let $H \leq S_m$ have index m . As with any subgroup, S_m acts transitively on the set of left cosets S_m/H by left multiplication, giving a group homomorphism

$$\varphi : S_m \rightarrow S_m;$$

the kernel $\ker(\varphi)$ is $K := \bigcap_{\sigma \in S_m} \sigma^{-1}H\sigma$, the core of H in S_m . In particular, K is a normal subgroup of S_m contained in H . Thus, K is either A_m or trivial, but if $K = A_m$, then $A_m \leq H$, so

$$\frac{m!}{2} \leq (m-1)! \iff m \leq 2.$$

Hence, φ is injective, and the restriction of φ to H is also injective. Dropping the singleton orbit $\{H\}$ from S_m still leaves an injective action.

Altogether, this gives a group embedding $H \hookrightarrow S_{m-1}$, hence an isomorphism $H \cong S_{m-1}$. This argument also shows that every such subgroup is obtained by fixing a single element of the set of m letters on which S_m acts. $\square$

Now we can prove Corollary 1.1.4:

Corollary 1.1.4. *Let $n \geq 7$ be odd. Then there is no strongly intersective polynomial of degree n whose factorisation shape is $(2, n-2)$ and whose Galois group is S_{n-2} .*

Proof. Let $m := n-2 \geq 5$. If such a polynomial were to exist, then we would need to conjugate-cover S_m by two subgroups, one of index 2 and one of index m . By standard group theory, the former must be A_m , and by Lemma 4.2.1, the latter is isomorphic to S_{m-1} obtained by fixing exactly one of the m letters on which S_m acts.

Now we claim that there is an odd permutation in S_{m-1} which has no fixed points, i.e., an odd derangement (see Definition 1.2.4). The existence of such an element would

complete the proof, as it cannot be conjugate to an element of A_m or an element of any copy of S_{m-1} in S_m .

Indeed, take the product of a disjoint 2-cycle and an $(m-2)$ -cycle. This is clearly a derangement, having length m with no 1-cycles. And, since m is odd, its sign is $(-1)^2(-1)^{m-2} = -1$, so it is not in A_m . □

We make another conjecture based on the conspicuous absence of the factorisation shape $(2, n-2)$ for even $n \geq 6$. The conjecture is stronger than Corollary 1.1.4 in that it does not assume a particular Galois group, but a different proof technique is required:

Conjecture 1.1.1. Let $n \geq 6$ be even. Then there is no strongly intersective polynomial of degree n with factorisation shape $(2, n-2)$.

Now for some observations and conjectural remarks concerning minimal intersectivity. Recall from Definition 1.1.1 that an intersective polynomial is called minimally intersective if none of its non-constant, proper divisors are intersective.

In many cases, it is easy to use Table C.1 to spot families of minimally intersective polynomials. For example, given a factorisation $(n_1, \dots, n_r)$, if none of the factorisations $(n_1, \dots, \widehat{n_i}, \dots, n_r)$ - which denotes the $(r-1)$ -tuple obtained by removing n_i - appear in the table, then any strongly intersective polynomials of this type must be minimal. This is obviously the case for any factorisation with $r = 2$, e.g., $(2, 7)$, but also with $(2, 2, 4)$, $(2, 3, 3)$, and $(2, 2, 6)$.

More interestingly, there are factorisations which are always minimal due to subdirect product constraints. For example, Table A.1 shows that C_2^3 (8.5) in the factorisation $(2, 2, 2, 2)$ is never a proper subdirect product of a product of three quadratics, so degree 8 is the lowest in which it can appear. The same is true for $C_2 \times D_6$ (24.14) in the factorisation $(2, 2, 2, 3)$.

Note that the above comments do not preclude other families in Table C.1 from being minimally intersective. While some given examples are clearly not minimal, e.g., the polynomial $(x^2 - 2)(x^2 - 17)(x^2 - 34)(x^2 - 68)$ with Galois group C_2^2 (4.2) which consists of a lower-degree example multiplied by a new factor, this says nothing about the *possibility* of constructing minimal examples.

References

- [1] R. Angelo and M. W. Xu. A polynomial with a root mod p for every p has a real root. *arXiv pre-print*, 2024. Accessed Feb. 10, 2025 via <https://arxiv.org/abs/2210.13735v2>.
- [2] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley, London, UK, 1969.
- [3] C. Awtrey, T. Cesarski, and P. Jakes. Determining Galois groups of reducible polynomials via discriminants and linear resolvents. *JP Journal of Algebra, Number Theory and Applications*, 39(5):685–702, 2017.
- [4] J. Ax. Solving Diophantine problems modulo every prime. *Annals of Mathematics*, 85(2):161–183, 1967.
- [5] N. Banks. Intersective-polynomials-algorithms. GitHub repository, 2025. Accessed Apr. 2, 2025 from <https://github.com/N2Banks/Intersective-Polynomials-Algorithms>.
- [6] L. Barreira and C. Valls. *Dynamical Systems: An Introduction*. Springer London, London, UK, 2012.
- [7] D. Berend and Y. Bilu. Polynomials with roots modulo every integer. *Proceedings of the American Mathematical Society*, 124(6):1663–1671, 1996.
- [8] V. Bergelson and I. J. Håland. Sets of recurrence and generalized polynomials. In V. Bergelson, P. March, and J. Rosenblatt, editors, *Convergence in Ergodic Theory and Probability*, pages 91–110. De Gruyter, Berlin, DE, 1996.
- [9] H. U. Besche, B. Eick, and E. A. O’Brien. The groups of order at most 2000. *Electronic Research Announcements of the American Mathematical Society*, 7:1–4, 2001.
- [10] M. Bhargava. Groups as unions of proper subgroups. *The American Mathematical Monthly*, 116(5):413–422, 2009.

- [11] M. A. Brodie, R. F. Chamberlain, and L.-C. Kappe. Finite coverings by normal subgroups. *Proceedings of the American Mathematical Society*, 104(3):239–258, 1988.
- [12] M. Bruckheimer, A. C. Bryan, and A. Muir. Groups which are the union of three subgroups. *The American Mathematical Monthly*, 77(1):57–52, 1970.
- [13] C. Carathéodory. Über den wiederkehrrsatz von Poincaré. *Berl. Sitzungsber*, pages 580–584, 1919.
- [14] A. Chenciner. Poincaré and the three-body problem. In B. Duplantier and V. Rivasseau, editors, *Henri Poincaré, 1912–2012*, chapter 2, pages 51–149. Birkhäuser Basel, Basel, CH, 2014.
- [15] S. Chidambaram. 18.782 - Introduction to Arithmetic Geometry. Lecture Notes, 2023. Accessed Nov. 02, 2025 from <https://math.mit.edu/classes/18.782/2023sp/lectures.html>.
- [16] H. Cohn. *A Classical Invitation to Algebraic Numbers and Class Fields*. Springer New York, New York, NY, 1978. With an appendix by Olga Taussky (R. Friedman, Trans.).
- [17] J. H. E. Cohn. On n -sum groups. *Mathematica Scandinavica*, 75(1):44–58, 1994.
- [18] K. Conrad. Discriminants and ramified primes. Expository Paper, n.d. Accessed Nov. 02, 2025 from <https://kconrad.math.uconn.edu/blurbs/gradnumthy/disc.pdf>.
- [19] K. Conrad. Galois groups over q and factorizations mod p . Expository Paper, n.d. Accessed Nov. 02, 2025 from <https://kconrad.math.uconn.edu/blurbs/gradnumthy/galois-Q-factor-mod-p.pdf>.
- [20] K. Conrad. History of class field theory. Expository Paper, n.d. Accessed Aug. 17, 2025 from <https://kconrad.math.uconn.edu/blurbs/gradnumthy/cfthistory.pdf>.
- [21] K. Conrad. Ostrowski for number fields. Expository Paper, n.d. Accessed Apr. 23, 2025 from <https://kconrad.math.uconn.edu/blurbs/gradnumthy/ostrowskinumbfield.pdf>.
- [22] K. Conrad. Rings of integers without a power basis. Expository Paper, n.d. Accessed Nov. 02, 2025 from <https://kconrad.math.uconn.edu/blurbs/gradnumthy/nopowerbasis.pdf>.
- [23] D. S. Dummit and R. M. Foote. *Abstract Algebra*. Wiley, Hoboken, NJ, 3rd edition, 2004.

- [24] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer-Verlag, New York, NY, 1995.
- [25] D. Ellis and S. Harper. Orbits of permutation groups with no derangements. *arXiv pre-print*, 2024. Accessed Apr. 14, 2025 via <https://arxiv.org/abs/2408.16064v2>.
- [26] C. Elsholtz, B. Klahn, and M. Technau. On polynomials with roots modulo almost all primes. *Acta Arithmetica*, 205:251–263, 2022.
- [27] M. Emerton. Galoisian sets of prime numbers. MathOverflow, 2025. Accessed July 16, 2025 from <https://mathoverflow.net/q/1238>.
- [28] B. Fein, W. M. Kantor, and M. Schacher. Relative Brauer groups II.. *Journal für die reine und angewandte Mathematik*, 328:39–57, 1981.
- [29] M. Fried and G. S. Sacerdote. Solving Diophantine problems over all residue class fields of a number field and all finite fields. *Annals of Mathematics*, 104(2):203–233, 1976.
- [30] H. Furstenberg. Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *Journal d’Analyse Mathématique*, 31:204–256, 1977.
- [31] H. Furstenberg. Poincaré recurrence and number theory. *Bulletin of the American Mathematical Society*, 5:211–234, 1981.
- [32] H. Furstenberg, Y. Katznelson, and D. Ornstein. The ergodic theoretical proof of Szemerédi’s theorem. *Bulletin of the American Mathematical Society*, 7:527–552, 1982.
- [33] D. Gorenstein. *The Classification of Finite Simple Groups*. Springer, Boston, MA, 1st edition, 1983.
- [34] D. Gorenstein. *Finite Groups*. American Mathematical Society, Providence, RI, 2nd reprinted edition, 2007.
- [35] B. Green. On arithmetic structures in dense sets of integers. *Duke Mathematical Journal*, 114:215–238, 2002.
- [36] B. Green, T. Tao, and T. Ziegler. A Fourier-free proof of the furstenberg-sarkozy theorem. Blog post, February 28, 2013. Accessed Feb. 2, 2025 from <https://terrytao.wordpress.com/2013/02/28/a-fourier-free-proof-of-the-furstenberg-sarkozy-theorem/>.

- [37] A. M. Hyde, P. D. Lee, and B. K. Spearman. Polynomials $(x^3 - n)(x^2 + 3)$ solvable modulo any integer. *The American Mathematical Monthly*, 121, 2014.
- [38] A. M. Hyde and B. K. Spearman. Products of quadratic polynomials with roots modulo any integer. *International Mathematical Forum*, 8:125–1231, 2013.
- [39] K. Igusa. Math 101b: Algebra II. Lecture Notes, 2009. Accessed Apr. 14, 2025 from https://people.brandeis.edu/~igusa/Math101bS07/Math101b_notesD3c.pdf.
- [40] I. M. Isaacs. *Character Theory of Finite Groups*. Academic Press, New York, NY, 1st edition, 1976.
- [41] T. Kamae and M. Mendès France. van der Corput’s difference theorem. *Israel Journal of Mathematics*, 31(3-4):335–342, 1978.
- [42] S. Lang. *Algebra*. Springer, New York, NY, 3rd edition, 2002.
- [43] H. Lenstra, Jr. and P. Stevenhagen. Chebotarëv and his density theorem. *The Mathematical Intelligencer*, 18(2):26–37, 1996.
- [44] LMFDB Collaboration. The L-functions and modular forms database. <https://www.lmfdb.org>, 2025. Accessed October 3rd, 2025 from <https://www.lmfdb.org>.
- [45] N. Lyall. A new proof of Sárközy’s theorem. *Proceedings of the American Mathematical Society*, 141(7):2253–2264, 2013.
- [46] D. A. Marcus. *Number Fields*. Springer, New York, NY, 2nd edition, 2018.
- [47] J. Milne. Algebraic number theory. Lecture notes, July 2020. Accessed Apr. 1, 2025 from <https://www.jmilne.org/math/CourseNotes/ANT.pdf>.
- [48] B. Mishra. Minimally intersective polynomials with arbitrarily long factorization. *Integers - Electronic Journal of Combinatorial Number Theory*, 22, 2022.
- [49] B. Mishra. Polynomials consisting of quadratic factors with roots modulo any positive integer. *The American Mathematical Monthly*, 129:178–182, 2022.
- [50] B. Mishra. Polynomials over ring of integers of global fields that have roots modulo every finite indexed subgroup. *Journal of Algebra*, 608:239–258, 2022.
- [51] J. Moreira. Equidistribution of polynomials, recurrence and van der Corput trick. Blog post, September 19, 2011. Accessed Feb. 3, 2025 from <https://joelmoreira.wordpress.com/2011/09/19/equidistribution-of-polynomials-recurrence-and-van-der-corput-trick/>.

- [52] J. Neukirch. *Algebraic Number Theory*. Springer, Berlin, DE, 1999.
- [53] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*. Springer, Berlin, DE, 5nd corr. print edition, 2008.
- [54] I. Niven, H. L. Montgomery, and H. S. Zuckerman. *An Introduction to the Theory of Numbers*. Wiley, New York, NY, 5th edition, 1991.
- [55] M. E. Pohst. A note on index divisors. In A. Pethö, M. E. Pohst, H. C. Williams, and H. G. Zimmer, editors, *Computational Number Theory: Proceedings of the Colloquium on Computational Number Theory held at Kossuth Lajos University, Debrecen (Hungary), September 4-9, 1989*, chapter 15, pages 173–182. Walter de Gruyter, Berlin, DE, 1991.
- [56] H. Poincaré. Sur le problème des trois corps et les équations de la dynamique. *Acta Mathematica*, 13:1–270, 1890.
- [57] rm50 (10146) (username). Krasner’s lemma. Expository notes, 2013. Accessed Apr. 1, 2025 from <https://planetmath.org/krasnerslemma>.
- [58] G. Scorza. I gruppi che possono pensarsi come somme di tre loro sottogruppi [groups that can be thought of as sums of three of their subgroups]. *Bollettino dell’Unione Matematica Italiana, Serie 1*, 5(5):216–218, 1926.
- [59] J.-P. Serre. *Linear Representations of Finite Groups*. Springer-Verlag, New York, NY, 1st edition, 1977.
- [60] J.-P. Serre. *Local Fields*. Springer-Verlag, New York, NY, 2nd corr. print edition, 1995.
- [61] J. Sonn. Polynomials with roots in $\mathbb{Q}_p$ for all p . *Proceedings of the American Mathematical Society*, 136(6):1955–1960, 2008.
- [62] J. Sonn. Two remarks on the inverse Galois problem for intersective polynomials. *Journal de Théorie des Nombres de Bordeaux*, 435-437(2):435–437, 2009.
- [63] M. M. Soule. A classification and study of intersective polynomials. Master’s thesis, San Diego State University, 2013.
- [64] A. Sárközy. On difference sets of sequences of integers. I. *Acta Mathematica Academiae Scientiarum Hungaricae*, 31(1-2):125–149, 1978.
- [65] M. J. Tomkinson. Groups as the union of proper subgroups. *Mathematica Scandinavica*, (81):191–198, 1997.

APPENDICES

Appendix A

Table of Subdirect Products for Products of Galois Groups

Table A.1: Proper subdirect products of direct products of Galois groups of degrees 5 to 10

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
Degree 5			
(2, 3)	$C_2 \times C_3$	None	
	$C_2 \times S_3$	S_3 (6.1)	
Degree 6			
(2, 2, 2)	$C_2 \times C_2 \times C_2$	C_2 (2.1)	
		C_2^2 (4.2)	
(2, 4)	$C_2 \times C_4$	C_4 (4.1)	
	$C_2 \times C_2^2$	C_2^2 (4.2)	
	$C_2 \times D_4$	D_4 (8.3)	
	$C_2 \times A_4$	None	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(2, 4)	$C_2 \times S_4$	S_4 (24.12)	
	$C_3 \times C_3$	C_3 (3.1)	
(3, 3)	$C_3 \times S_3$	None	
	$S_3 \times S_3$	S_3 (6.1) $C_3 : S_3$ (18.4)	
Degree 7			
(2, 2, 3)	$C_2 \times C_2 \times C_3$	C_6 (6.2)	
	$C_2 \times C_2 \times S_3$	S_3 (6.1) D_6 (12.4)	
	$C_2 \times C_5$	None	
(2, 5)	$C_2 \times D_5$	D_5 (10.1)	
	$C_2 \times F_5$	F_5 (20.3)	
	$C_2 \times A_5$	None	
	$C_2 \times S_5$	S_5 (120.34)	
	$C_3 \times C_4$	None	
	$C_3 \times C_2^2$	None	
	$C_3 \times D_4$	None	
(3, 4)	$C_3 \times A_4$	A_4 (12.3)	
	$C_3 \times S_4$	None	
	$S_3 \times C_4$	$C_3 : C_4$ (12.1)	
	$S_3 \times C_2^2$	D_6 (12.4)	
	$S_3 \times D_4$	D_{12} (24.6) $C_3 : D_4$ (24.8)	
	$S_3 \times A_4$	None	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(3, 4)	$S_3 \times S_4$	S_4 (24.12) $C_3 : S_4$ (72.43)	
Degree 8			
(2, 2, 2, 2)	$C_2 \times C_2 \times C_2 \times C_2$	C_2 (2.1) C_2^2 (4.2) C_2^3 (8.5)	
(2, 3, 3)	$C_2 \times C_3 \times C_3$	C_6 (6.2)	
	$C_2 \times C_3 \times S_3$	$C_3 \times S_3$ (18.3)	
	$C_2 \times S_3 \times S_3$	S_3 (6.1) D_6 (12.4) $C_3 : S_3$ (18.4) S_3^2 (36.10) $C_6 : S_3$ (36.13)	
	$C_2 \times C_2 \times C_4$	C_4 (4.1) $C_2 \times C_4$ (8.2)	
	$C_2 \times C_2 \times C_2^2$	C_2^2 (4.2) C_2^3 (8.5)	
(2, 2, 4)	$C_2 \times C_2 \times D_4$	D_4 (8.3) $C_2 \times D_4$ (16.11)	
(2, 2, 4)	$C_2 \times C_2 \times A_4$	$C_2 \times A_4$ (24.13)	
	$C_2 \times C_2 \times S_4$	S_4 (24.12) $C_2 \times S_4$ (48.48)	
	$C_4 \times C_4$	C_4 (4.1) $C_2 \times C_4$ (8.2)	
(4, 4)	$C_4 \times C_2^2$	$C_2 \times C_4$ (8.2)	
(4, 4)	$C_4 \times D_4$	$C_2^2 : C_4$ (16.3) $C_4 : C_4$ (16.4)	
	$C_4 \times A_4$	None	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(4, 4)	$C_4 \times S_4$	$A_4 : C_4$ (48.30)	
	$C_2^2 \times C_2^2$	C_2^2 (4.2) C_2^3 (8.5)	
	$C_2^2 \times D_4$	D_4 (8.3) $C_2 \times D_4$ (16.11)	
	$C_2^2 \times A_4$	None	
	$C_2^2 \times S_4$	$C_2 \times S_4$ (48.48)	
	$D_4 \times D_4$	D_4 (8.3) $C_2^2 : C_4$ (16.3) $C_2 \times D_4$ (16.11) $C_2^2 \wr C_2$ (32.27) $C_4 : D_4$ (32.28 and 32.34)	
	$D_4 \times A_4$	None	
	$D_4 \times S_4$	$C_4 : S_4$ (96.187) $\text{GL}(2, \mathbb{Z}/4)$ (96.195)	
	$A_4 \times A_4$	A_4 (12.3) $C_2^2 : A_4$ (48.50)	
	$A_4 \times S_4$	None	
	$S_4 \times S_4$	S_4 (24.12) $C_2^2 : S_4$ (96.227) $\text{PSO}^+(4, 3)$ (288.1026)	
(2, 2, 4)	$C_2 \times C_2 \times C_4$	C_4 (4.1) $C_2 \times C_4$ (8.2)	
	$C_2 \times C_2 \times C_2^2$	C_2^2 (4.2) C_2^3 (8.5)	
	$C_2 \times C_2 \times D_4$	D_4 (8.3) $C_2 \times D_4$ (16.11)	
	$C_2 \times C_2 \times A_4$	$C_2 \times A_4$ (24.13)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(2, 2, 4)	$C_2 \times C_2 \times S_4$	S_4 (24.12)	
		$C_2 \times S_4$ (48.48)	
(3, 5)	$C_3 \times C_5$	None	
	$C_3 \times D_5$	None	
	$C_3 \times F_5$	None	
	$C_3 \times A_5$	None	
	$C_3 \times S_5$	None	
	$S_3 \times C_5$	None	
	$S_3 \times D_5$	D_{15} (30.3)	
	$S_3 \times F_5$	$C_{15} : C_4$ (60.7)	
	$S_3 \times A_5$	None	
	$S_3 \times S_5$	$C_3 : S_5$ (360.120)	
(2, 6)	$C_2 \times C_6$	C_6 (6.2)	
	$C_2 \times S_3$	S_3 (6.1)	
	$C_2 \times D_6$	D_6 (12.4)	
	$C_2 \times A_4$	None	
	$C_2 \times (C_3 \times S_3)$	$C_3 \times S_3$ (18.3)	
	$C_2 \times (C_2 \times A_4)$	$C_2 \times A_4$ (24.13)	
	$C_2 \times S_4$	S_4 (24.12)	
	$C_2 \times S_3^2$	S_3^2 (36.10)	
	$C_2 \times (C_3^2 : C_4)$	$C_3^2 : C_4$ (36.9)	
	$C_2 \times (C_2 \times S_4)$	$C_2 \times S_4$ (48.48)	
	$C_2 \times A_5$	None	
	$C_2 \times \text{SO}^+(4, 2)$	$\text{SO}^+(4, 2)$ (72.40)	
	$C_2 \times S_5$	S_5 (120.34)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(2, 6)	$C_2 \times A_6$	None	
	$C_2 \times S_6$	S_6 (720.763)	
Degree 9			
(2, 2, 2, 3)	$C_2 \times C_2 \times C_2 \times C_3$	C_6 (6.2) $C_2 \times C_6$ (12.5)	
	$C_2 \times C_2 \times C_2 \times S_3$	S_3 (6.1) D_6 (12.4) $C_2 \times D_6$ (24.14)	
	$C_3 \times C_3 \times C_3$	C_3 (3.1) C_3^2 (9.2)	
	$C_3 \times C_3 \times S_3$	$C_3 \times S_3$ (18.3)	
(3, 3, 3)	$C_3 \times S_3 \times C_3$	$C_3 \times S_3$ (18.3) $C_3^2 : C_6$ (54.13)	
	$S_3 \times S_3 \times S_3$	S_3 (6.1) $C_3 : S_3$ (18.4) S_3^2 (36.10) $C_3^2 : S_3$ (54.14) $C_3 : S_3^2$ (108.39) $C_3 : S_3^2$ (108.40)	
(2, 3, 4)	$C_2 \times C_3 \times C_4$	C_{12} (12.2)	
	$C_2 \times C_3 \times C_2^2$	$C_2 \times C_6$ (12.5)	
	$C_2 \times C_3 \times D_4$	$C_3 \times D_4$ (24.10)	
	$C_2 \times C_3 \times A_4$	$C_2 \times A_4$ (24.13)	
	$C_2 \times C_3 \times S_4$	$C_3 \times S_4$ (72.42)	
	$C_2 \times S_3 \times C_4$	$C_3 : C_4$ (12.1) $C_4 \times S_3$ (24.5) $C_6 : C_4$ (24.7)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(2, 3, 4)	$C_2 \times S_3 \times C_2^2$	D_6 (12.4) $C_2 \times D_6$ (24.14)	
	$C_2 \times S_3 \times D_4$	D_{12} (24.6) $C_3 : D_4$ (24.8) $C_2 \times D_{12}$ (48.36) $S_3 \times D_4$ (48.38) $C_6 : D_4$ (48.43)	
	$C_2 \times S_3 \times A_4$	$S_3 \times A_4$ (72.44)	
	$C_2 \times S_3 \times S_4$	S_4 (24.12) $C_2 \times S_4$ (48.48) $C_3 : S_4$ (72.43) $S_3 \times S_4$ (144.183) $C_6 : S_4$ (144.189)	
(2, 2, 5)	$C_2 \times C_2 \times C_5$	C_{10} (10.2)	
	$C_2 \times C_2 \times D_5$	D_5 (10.1) D_{10} (20.4)	
	$C_2 \times C_2 \times F_5$	F_5 (20.3) $C_2 \times F_5$ (40.12)	
	$C_2 \times C_2 \times A_5$	$C_2 \times A_5$ (120.35)	
	$C_2 \times C_2 \times S_5$	S_5 (120.34) $C_2 \times S_5$ (240.189)	
(4, 5)	$C_4 \times C_5$	None	
	$C_4 \times D_5$	$C_5 : C_4$ (20.1)	
	$C_4 \times F_5$	F_5 (20.3) $C_2 \times F_5$ (40.12)	
	$C_4 \times A_5$	None	
	$C_4 \times S_5$	$A_5 : C_4$ (240.91)	
	$C_2^2 \times C_5$	None	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(4, 5)	$C_2^2 \times D_5$	D_{10} (20.4)	
	$C_2^2 \times F_5$	$C_2 \times F_5$ (40.12)	
	$C_2^2 \times A_5$	None	
	$C_2^2 \times S_5$	$C_2 \times S_5$ (240.189)	
	$D_4 \times C_5$	None	
	$D_4 \times D_5$	D_{20} (40.6) $C_5 : D_4$ (40.8)	
	$D_4 \times F_5$	$C_{20} : C_4$ (80.31) $(C_{10} \times C_2) : C_4$ (80.34)	
	$D_4 \times A_5$	None	
	$D_4 \times S_5$	$C_4 : S_5$ (480.944) $C_2^2 : S_5$ (480.951)	
	$A_4 \times C_5$	None	
	$A_4 \times D_5$	None	
	$A_4 \times F_5$	None	
	$A_4 \times A_5$	None	
	$A_4 \times S_5$	None	
	$S_4 \times C_5$	None	
	$S_4 \times D_5$	$C_5 : S_4$ (120.38)	
	$S_4 \times F_5$	$C_5 : (A_4 : C_4)$ (240.192)	
	$S_4 \times A_5$	None	
	$S_4 \times S_5$	$A_4 : S_5$ (1440.5847)	
(3, 6)	$C_3 \times C_6$	C_6 (6.2)	
	$C_3 \times S_3$	None	
	$C_3 \times D_6$	None	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(3, 6)	$C_3 \times A_4$	A_4 (12.3)	
	$C_3 \times (C_3 \times S_3)$	$C_3 \times S_3$ (18.3)	
	$C_3 \times (C_2 \times A_4)$	$C_2 \times A_4$ (24.13)	
	$C_3 \times S_4$	None	
	$C_3 \times S_3^2$	None	
	$C_3 \times (C_3^2 : C_4)$	None	
	$C_3 \times (C_2 \times S_4)$	None	
	$C_3 \times A_5$	None	
	$C_3 \times \text{SO}^+(4, 2)$	None	
	$C_3 \times S_5$	None	
	$C_3 \times A_6$	None	
	$C_3 \times S_6$	None	
	$S_3 \times C_6$	$C_3 \times S_3$ (18.3)	
	$S_3 \times S_3$	S_3 (6.1) $C_3 : S_3$ (18.4)	
	$S_3 \times D_6$	D_6 (12.4) S_3^2 (36.10) $C_6 : S_3$ (36.13)	
	$S_3 \times A_4$	None	
	$S_3 \times (C_3 \times S_3)$	$C_3 \times S_3$ (18.3) $C_3^2 : C_6$ (54.13)	
	$S_3 \times (C_2 \times A_4)$	$S_3 \times A_4$ (72.44)	
	$S_3 \times S_4$	S_4 (24.12) $C_3 : S_4$ (72.43)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(3, 6)	$S_3 \times S_3^2$	S_3^2 (36.10) $S_3 \times (C_3^2 : C_2)$ (108.39) $C_3 : S_3^2$ (108.40)	
	$S_3 \times (C_3^2 : C_4)$	$C_3^3 : C_4$ (108.37)	
	$S_3 \times (C_2 \times S_4)$	$C_2 \times S_4$ (48.48) $S_3 \times S_4$ (144.183) $C_6 : S_4$ (144.189)	
	$S_3 \times A_5$	None	
	$S_3 \times \text{SO}^+(4, 2)$	$S_3^2 : S_3$ (216.158) $C_3^2 : D_{12}$ (216.159)	
	$S_3 \times S_5$	$C_3 : S_5$ (360.120)	
	$S_3 \times A_6$	None	
	$S_3 \times S_6$	$C_3 : S_6$ (2160.cb)	
(2, 7)	$C_2 \times C_7$	None	
	$C_2 \times D_7$	D_7 (14.1)	
	$C_2 \times (C_7 : C_3)$	None	
	$C_2 \times F_7$	F_7 (42.1)	
	$C_2 \times \text{GL}(3, 2)$	None	
	$C_2 \times A_7$	None	
	$C_2 \times S_7$	S_7 (5040.w)	
Degree 10			
(2, 2, 2, 2)	$C_2 \times C_2 \times C_2 \times C_2 \times C_2$	C_2 (2.1) C_2^2 (4.2) C_2^3 (8.5) C_2^4 (16.14)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(2, 2, 2, 4)	$C_2 \times C_2 \times C_2 \times C_4$	C_4 (4.1)	
		$C_2 \times C_4$ (8.2)	
		$C_2^2 \times C_4$ (16.10)	
	$C_2 \times C_2 \times C_2 \times C_2^2$	C_2^2 (4.2)	
		C_2^3 (8.5)	
		C_2^4 (16.14)	
(2, 2, 2, 4)	$C_2 \times C_2 \times C_2 \times D_4$	D_4 (8.3)	
		$C_2 \times D_4$ (16.11)	
		$C_2^2 \times D_4$ (32.46)	
	$C_2 \times C_2 \times C_2 \times A_4$	$C_2 \times A_4$ (24.13)	
		$C_2^2 \times A_4$ (48.49)	
	$C_2 \times C_2 \times C_2 \times S_4$	S_4 (24.12)	
		$C_2 \times S_4$ (48.48)	
		$C_2^2 \times S_4$ (96.226)	
(2, 2, 3, 3)	$C_2 \times C_2 \times C_3 \times C_3$	C_6 (6.2)	
		$C_2 \times C_6$ (12.5)	
		$C_3 \times C_6$ (18.5)	
	$C_2 \times C_2 \times C_3 \times S_3$	$C_3 \times S_3$ (18.3)	
		$C_6 \times S_3$ (36.12)	
	$C_2 \times C_2 \times S_3 \times S_3$	S_3 (6.1)	
		D_6 (12.4)	
		$C_3 : S_3$ (18.4)	
		$C_2 \times D_6$ (24.14)	
		S_3^2 (36.10)	
		$C_6 : S_3$ (36.13)	
		$S_3 \times D_6$ (72.46)	
		$C_6 : D_6$ (72.49)	
(2, 2, 6)	$C_2 \times C_2 \times C_6$	C_6 (6.2)	
		$C_2 \times C_6$ (12.5)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(2, 2, 6)	$C_2 \times C_2 \times S_3$	S_3 (6.1) D_6 (12.4)	
	$C_2 \times C_2 \times D_6$	D_6 (12.4) $C_2 \times D_6$ (24.14)	
	$C_2 \times C_2 \times A_4$	$C_2 \times A_4$ (24.13)	
	$C_2 \times C_2 \times (C_3 \times S_3)$	$C_3 \times S_3$ (18.3) $C_6 \times S_3$ (36.12)	
	$C_2 \times C_2 \times (C_2 \times A_4)$	$C_2 \times A_4$ (24.13) $C_2^2 \times A_4$ (48.49)	
	$C_2 \times C_2 \times S_4$	S_4 (24.12) $C_2 \times S_4$ (48.48)	
	$C_2 \times C_2 \times S_3^2$	S_3^2 (36.10) $S_3 \times D_6$ (72.46)	
	$C_2 \times C_2 \times (C_3^2 : C_4)$	$C_3^2 : C_4$ (36.9) $C_2 \times (C_3^2 : C_4)$ (72.45)	
	$C_2 \times C_2 \times (C_2 \times S_4)$	$C_2 \times S_4$ (48.48) $C_2^2 \times S_4$ (96.226)	
	$C_2 \times C_2 \times A_5$	$C_2 \times A_5$ (120.35)	
	$C_2 \times C_2 \times \text{SO}^+(4, 2)$	$\text{SO}^+(4, 2)$ (72.40) $S_3^2 : C_2^2$ (144.186)	
	$C_2 \times C_2 \times S_5$	S_5 (120.34) $C_2 \times S_5$ (240.189)	
	$C_2 \times C_2 \times A_6$	$C_2 \times A_6$ (720.766)	
	$C_2 \times C_2 \times S_6$	S_6 (720.763) $C_2 \times S_6$ (1440.5842)	
(2, 3, 5)	$C_2 \times C_3 \times C_5$	None	
	$C_2 \times C_3 \times D_5$	$C_3 \times D_5$ (30.2)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(2, 3, 5)	$C_2 \times C_3 \times F_5$	$C_3 \times F_5$ (60.6)	
	$C_2 \times C_3 \times A_5$	None	
	$C_2 \times C_3 \times S_5$	$C_3 \times S_5$ (360.119)	
	$C_2 \times S_3 \times C_5$	$C_5 \times S_3$ (30.1)	
	$C_2 \times S_3 \times D_5$	D_{15} (30.3) $S_3 \times D_5$ (60.8) D_{30} (60.12)	
	$C_2 \times S_3 \times F_5$	$C_{15} : C_4$ (60.7) $S_3 \times F_5$ (120.36) $C_{30} : C_4$ (120.41)	
	$C_2 \times S_3 \times A_5$	$S_3 \times A_5$ (360.121)	
	$C_2 \times S_3 \times S_5$	$C_3 : S_5$ (360.120) $S_3 \times S_5$ (720.767) $C_6 : S_5$ (720.770)	
	$C_2 \times C_4 \times C_4$	C_4 (4.1) $C_2 \times C_4$ (8.2) C_4^2 (16.2) $C_2^2 \times C_4$ (16.10)	
	$C_2 \times C_4 \times C_2^2$	$C_2 \times C_4$ (8.2) $C_2^2 \times C_4$ (16.10)	
(2, 4, 4)	$C_2 \times C_4 \times D_4$	$C_2^2 : C_4$ (16.3) $C_4 : C_4$ (16.4) $C_2^3 : C_4$ (32.22) $C_2^2.D_4$ (32.23) $C_4 \times D_4$ (32.25)	
	$C_2 \times C_4 \times A_4$	$C_4 \times A_4$ (48.31)	
	$C_2 \times C_4 \times S_4$	$A_4 : C_4$ (48.30) $C_4 \times S_4$ (96.186) $C_2^2.S_4$ (96.194)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(2, 4, 4)	$C_2 \times C_2^2 \times C_2^2$	C_2^2 (4.2) C_2^3 (8.5) C_2^4 (16.14)	
	$C_2 \times C_2^2 \times D_4$	D_4 (8.3) $C_2 \times D_4$ (16.11) $C_2^2 \times D_4$ (32.46)	
	$C_2 \times C_2^2 \times A_4$	$C_2^2 \times A_4$ (48.49)	
	$C_2 \times C_2^2 \times S_4$	$C_2 \times S_4$ (48.48) $C_2^2 \times S_4$ (96.226)	
	$C_2 \times D_4 \times D_4$	D_4 (8.3) $C_2^2 : C_4$ (16.3) $C_2 \times D_4$ (16.11) $C_2^3 : C_4$ (32.22) $C_2^2 \wr C_2$ (32.27) $C_4 : D_4$ (32.28 and 32.34) $C_2^2 \times D_4$ (32.46) $C_2^3 : D_4$ (64.202 and 64.203) $C_4^2 : C_2^2$ (64.211) D_4^2 (64.226)	
	$C_2 \times D_4 \times A_4$	$D_4 \times A_4$ (96.197)	
	$C_2 \times D_4 \times S_4$	$C_4 : S_4$ (96.187) $\text{GL}(2, \mathbb{Z}/4)$ (96.195) $C_2^3 : D_{12}$ (192.1470) $D_4 \times S_4$ (192.1472) $C_2 \times \text{GL}(2, \mathbb{Z}/4)$ (192.1488)	
	$C_2 \times A_4 \times A_4$	$C_2 \times A_4$ (24.13) $C_2^3 : A_4$ (96.229)	
	$C_2 \times A_4 \times S_4$	$A_4 \times S_4$ (288.1024)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(2, 4, 4)	$C_2 \times S_4 \times S_4$	S_4 (24.12) $C_2 \times S_4$ (48.48) $C_2^2 : S_4$ (96.227) $C_2^3 : S_4$ (192.1538) $\text{PSO}^+(4, 3)$ (288.1026) S_4^2 (576.8653) $A_4^2 : C_2^2$ (576.8657)	
	$C_2 \times C_8$	C_8 (8.1)	
	$C_2 \times (C_2 \times C_4)$	$C_2 \times C_4$ (8.2)	
	$C_2 \times C_2^3$	C_2^3 (8.5)	
	$C_2 \times D_4$	D_4 (8.3)	
	$C_2 \times Q_8$	Q_8 (8.4)	
	$C_2 \times D_8$	D_8 (16.7)	
(2, 8)	$C_2 \times \text{OD}_{16}$	OD_{16} (16.6)	
	$C_2 \times \text{SD}_{16}$	SD_{16} (16.8)	
	$C_2 \times (C_2 \times D_4)$	$C_2 \times D_4$ (16.11)	
	$C_2 \times (C_2^2 : C_4)$	$C_2^2 : C_4$ (16.3)	
	$C_2 \times (Q_8 : C_2)$	$D_4 : C_2$ (16.13)	
	$C_2 \times \text{SL}(2, 3)$	None	
	$C_2 \times (C_2 \times A_4)$	$C - 2 \times A_4$ (24.13)	
	$C_2 \times S_4$	S_4 (24.12)	
	$C_2 \times (D_8 : C_2)$	$D_8 : C_2$ (32.43)	
	$C_2 \times (\text{OD}_{16} : C_2)$	$\text{OD}_{16} : C_2$ (32.7)	
	$C_2 \times (C_4 \wr C_2)$	$C_4 \wr C_2$ (32.11)	
	$C_2 \times (C_2^2 \wr C_2)$	$C_2^2 \wr C_2$ (32.27)	
	$C_2 \times (C_2^3 : C_4)$	$C_2^3 : C_4$ (32.6)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(2, 8)	$C_2 \times (D_4 : C_2^2)$	$D_4 : C_2^2$ (32.49)	
	$C_2 \times \text{GL}(2, 3)$	$\text{GL}(2, 3)$ (48.29)	
	$C_2 \times (C_2 \times S_4)$	$C_2 \times S_4$ (48.48)	
	$C_2 \times (C_2^3 : C_7)$	None	
	$C_2 \times (D_4 : D_4)$	$D_4 : D_4$ (64.134)	
	$C_2 \times (C_2 \wr C_4)$	$C_2 \wr C_4$ (64.32)	
	$C_2 \times (C_2 \wr C_2^2)$	$C_2 \wr C_2^2$ (64.138)	
	$C_2 \times (C_4^2 : C_4)$	$C_4^2 : C_4$ (64.34)	
	$C_2 \times (Q_8 : A_4)$	None	
	$C_2 \times (C_2^4 : C_6)$	$C_2^4 : C_6$ (96.70)	
	$C_2 \times (C_2^2 : S_4)$	$C_2^2 : S_4$ (96.227)	
	$C_2 \times (C_2 \wr D_4)$	$C_2 \wr D_4$ (128.928)	
	$C_2 \times (F_8 : C_3)$	None	
	$C_2 \times \text{GL}(3, 2)$	None	
	$C_2 \times (C_2 \wr A_4)$	$C_2 \wr A_4$ (192.201)	
	$C_2 \times (C_2^3 : S_4)$	$C_2^3 : S_4$ (192.1493)	
	$C_2 \times (Q_8 : S_4)$	$Q_8 : S_4$ (192.1494)	
	$C_2 \times (C_2^4 : D_6)$	$C_2^4 : D_6$ (192.955)	
	$C_2 \times (A_4 \wr C_2)$	$A_4 \wr C_2$ (288.1025)	
	$C_2 \times \text{PGL}(2, 7)$	$\text{PGL}(2, 7)$ (336.208)	
	$C_2 \times (C_2 \wr S_4)$	$C_2 \wr S_4$ (384.5602)	
	$C_2 \times \text{PGO}^+(4, 3)$	$\text{PGO}^+(4, 3)$ (576.8654)	
	$C_2 \times (A_4^2 : C_4)$	$A_4^2 : C_4$ (576.8652)	
	$C_2 \times (S_4 \wr C_2)$	$S_4 \wr C_2$ (1152.157849)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(2, 8)	$C_2 \times (C_2^3 : \text{GL}(3, 2))$	None	
	$C_2 \times A_8$	None	
	$C_2 \times S_8$	S_8 (40320.a)	
(3, 3, 4)	$C_3 \times C_3 \times C_4$	C_{12} (12.2)	
	$C_3 \times C_3 \times C_2^2$	$C_2 \times C_6$ (12.5)	
	$C_3 \times C_3 \times D_4$	$C_3 \times D_4$ (24.10)	
	$C_3 \times C_3 \times A_4$	A_4 (12.3) $C_3 \times A_4$ (36.11)	
	$C_3 \times C_3 \times S_4$	$C_3 \times S_4$ (72.42)	
	$C_3 \times S_3 \times C_4$	$C_3 : C_{12}$ (36.6)	
	$C_3 \times S_3 \times C_2^2$	$C_6 \times S_3$ (36.12)	
	$C_3 \times S_3 \times D_4$	$C_3 \times D_{12}$ (72.28) $C_6 \wr C_2$ (72.30)	
	$C_3 \times S_3 \times A_4$	$S_3 \times A_4$ (72.44)	
	$C_3 \times S_3 \times S_4$	$C_3 \times S_4$ (72.42) $C_3^2 : S_4$ (216.164)	
	$S_3 \times S_3 \times C_4$	$C_3 : C_4$ (12.1) $C_4 \times S_3$ (24.5) $C_3^2 : C_4$ (36.7) $C_6.D_6$ (72.20 and 72.21) $C_{12} : S_3$ (72.32)	
	$S_3 \times S_3 \times C_2^2$	D_6 (12.4) $C_2 \times D_6$ (24.14) S_3^2 (36.10) $C_6 : S_3$ (36.13) $S_3 \times D_6$ (72.46) $C_6 : D_6$ (72.49)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(3, 3, 4)	$S_3 \times S_3 \times D_4$	D_{12} (24.6)	
		$C_3 : D_4$ (24.8)	
		$S_3 \times D_4$ (48.38)	
		$D_6 : S_3$ (72.22)	
		$C_3 : D_{12}$ (72.23)	
		$C_3 : D_{12}$ (72.33)	
		$C_6^2 : C_2$ (72.35)	
		$S_3 \times D_{12}$ (144.144)	
		$C_{12} : D_6$ (144.145)	
		$D_6 : D_6$ (144.153)	
		$D_6 : D_6$ (144.154)	
		$C_{12} : D_6$ (144.172)	
(3, 3, 4)	$S_3 \times S_3 \times A_4$	$S_3 \times A_4$ (72.44)	
		$C_6^2 : C_6$ (216.167)	
	$S_3 \times S_3 \times S_4$	S_4 (24.12)	
		$C_3 : S_4$ (72.43)	
		$S_3 \times S_4$ (144.183)	
		$C_3^2 : S_4$ (216.165)	
		$C_6^2 : D_6$ (432.746)	
		$A_4 : S_3^2$ (432.747)	
		$A_4 : S_3^2$ (432.748)	
(3, 7)	$C_3 \times C_7$	None	
	$C_3 \times D_7$	None	
	$C_3 \times (C_7 : C_3)$	$C_7 : C_3$ (21.1)	
	$C_3 \times F_7$	F_7 (42.1)	
	$C_3 \times \text{GL}(3, 2)$	None	
	$C_3 \times A_7$	None	
	$C_3 \times S_7$	None	
	$S_3 \times C_7$	None	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(3, 7)	$S_3 \times D_7$	D_{21} (42.5)	
	$S_3 \times (C_7 : C_3)$	None	
	$S_3 \times F_7$	$C_{21} : C_6$ (126.9)	
	$S_3 \times \text{GL}(3, 2)$	None	
	$S_3 \times A_7$	None	
	$S_3 \times S_7$	$C_3 : S_7$ (15120.f)	
(4, 6)	$C_4 \times C_6$	C_{12} (12.2)	
	$C_4 \times S_3$	$C_3 : C_4$ (12.1)	
	$C_4 \times D_6$	$C_4 \times S_3$ (24.5) $C_6 : C_4$ (24.7)	
	$C_4 \times A_4$	None	
	$C_4 \times (C_3 \times S_3)$	$C_3 : C_{12}$ (36.6)	
	$C_4 \times (C_2 \times A_4)$	$C_4 \times A_4$ (48.31)	
	$C_4 \times S_4$	$A_4 : C_4$ (48.30)	
	$C_4 \times S_3^2$	$C_6.D_6$ (72.20 and 72.21)	
	$C_4 \times (C_3^2 : C_4)$	$C_3^2 : C_4$ (36.9) $C_2 \times (C_3^2 : C_4)$ (72.45)	
	$C_4 \times (C_2 \times S_4)$	$C_4 \times S_4$ (96.186) $C_2^2.S_4$ (96.194)	
	$C_4 \times A_5$	None	
	$C_4 \times \text{SO}^+(4, 2)$	$S_3^2 : C_4$ (144.115) $C_2.\text{SO}^+(4, 2)$ (144.116)	
	$C_4 \times S_5$	$A_5 : C_4$ (240.91)	
	$C_4 \times A_6$	None	
	$C_4 \times S_6$	$A_6 : C_4$ (1440.4590)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(4, 6)	$C_2^2 \times C_6$	$C_2 \times C_6$ (12.5)	
	$C_2^2 \times S_3$	D_6 (12.4)	
	$C_2^2 \times D_6$	D_6 (12.4) $C_2 \times D_6$ (24.14)	
	$C_2^2 \times A_4$	None	
	$C_2^2 \times (C_3 \times S_3)$	$C_6 \times S_3$ (36.12)	
	$C_2^2 \times (C_2 \times A_4)$	$C_2^2 \times A_4$ (48.49)	
	$C_2^2 \times S_4$	$C_2 \times S_4$ (48.48)	
	$C_2^2 \times S_3^2$	S_3^2 (36.10) $S_3 \times D_6$ (72.46)	
	$C_2^2 \times (C_3^2 : C_4)$	$C_2 \times (C_3^2 : C_4)$ (72.45)	
	$C_2^2 \times (C_2 \times S_4)$	$C_2 \times S_4$ (48.48) $C_2^2 \times S_4$ (96.226)	
	$C_2^2 \times A_5$	None	
	$C_2^2 \times \text{SO}^+(4, 2)$	$\text{SO}^+(4, 2)$ (72.40) $S_3^2 : C_2^2$ (144.186)	
	$C_2^2 \times S_5$	$C_2 \times S_5$ (240.189)	
	$C_2^2 \times A_6$	None	
	$C_2^2 \times S_6$	$C_2 \times S_6$ (1440.5842)	
	$D_4 \times C_6$	$C_3 \times D_4$ (24.10)	
	$D_4 \times S_3$	D_{12} (24.6) $C_3 : D_4$ (24.8)	
	$D_4 \times D_6$	D_{12} (24.6) $C_3 : D_4$ (24.8) $C_2 \times D_{12}$ (48.36) $S_3 \times D_4$ (48.38) $C_6 : D_4$ (48.43)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(4, 6)	$D_4 \times A_4$	None	
	$D_4 \times (C_3 \times S_3)$	$C_3 \times D_{12}$ (72.28) $C_6 \wr C_2$ (72.30)	
	$D_4 \times (C_2 \times A_4)$	$D_4 \times A_4$ (96.197)	
	$D_4 \times S_4$	$C_4 : S_4$ (96.187) $\mathrm{GL}(2, \mathbb{Z}/4)$ (96.195)	
	$D_4 \times S_3^2$	$D_6 : S_3$ (72.22) $C_3 : D_{12}$ (72.23) $S_3 \times D_{12}$ (144.144) $C_{12} : D_6$ (144.145) $D_6 : D_6$ (144.153 and 144.154)	
	$D_4 \times (C_3^2 : C_4)$	$(C_3 \times C_{12}) : C_4$ (144.133) $C_6^2 : C_4$ (144.136)	
	$D_4 \times (C_2 \times S_4)$	$C_4 : S_4$ (96.187) $\mathrm{GL}(2, \mathbb{Z}/4)$ (96.195) $C_2^3 : D_{12}$ (192.1470) $D_4 \times S_4$ (192.1472) $C_2 \times \mathrm{GL}(2, \mathbb{Z}/4)$ (192.1488)	
	$D_4 \times A_5$	None	
	$D_4 \times \mathrm{SO}^+(4, 2)$	$\mathrm{SO}^+(4, 2)$ (72.40) $S_3^2 : C_4$ (144.115) $S_3^2 : C_2^2$ (144.186) $S_3^2 : D_4$ (288.878) $C_4 : \mathrm{SO}^+(4, 2)$ (288.879) $D_6 \wr C_2$ (288.889) $C_6^2 : D_4$ (288.890)	
	$D_4 \times S_5$	$C_4 : S_5$ (480.944) $C_2^2 : S_5$ (480.951)	
	$D_4 \times A_6$	None	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(4, 6)	$D_4 \times S_6$	$C_2^2 : S_6$ (2880.ea) $C_4 : S_6$ (2880.ec)	
	$A_4 \times C_6$	$C_2 \times A_4$ (24.13)	
	$A_4 \times S_3$	None	
	$A_4 \times D_6$	None	
	$A_4 \times A_4$	A_4 (12.3) $C_2^2 : A_4$ (48.50)	
	$A_4 \times (C_3 \times S_3)$	$S_3 \times A_4$ (72.44)	
	$A_4 \times (C_2 \times A_4)$	$C_2 \times A_4$ (24.13) $C_2^3 : A_4$ (96.229)	
	$A_4 \times S_4$	None	
	$A_4 \times S_3^2$	None	
	$A_4 \times (C_3^2 : C_4)$	None	
	$A_4 \times (C_2 \times S_4)$	None	
	$A_4 \times A_5$	None	
	$A_4 \times \text{SO}^+(4, 2)$	None	
	$A_4 \times S_5$	None	
	$A_4 \times A_6$	None	
	$A_4 \times S_6$	None	
	$S_4 \times C_6$	$C_3 \times S_4$ (72.42)	
	$S_4 \times S_3$	S_4 (24.12) $C_3 : S_4$ (72.43)	
	$S_4 \times D_6$	$C_2 \times S_4$ (48.48) $S_3 \times S_4$ (144.183) $C_6 : S_4$ (144.189)	
	$S_4 \times A_4$	None	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(4, 6)	$S_4 \times (C_3 \times S_3)$	$C_3 \times S_4$ (72.42) $C_3^2 : S_4$ (216.164)	
	$S_4 \times (C_2 \times A_4)$	$A_4 \times S_4$ (288.1024)	
	$S_4 \times S_4$	S_4 (24.12) $C_2^2 : S_4$ (96.227) $\text{PSO}^+(4, 3)$ (288.1026)	
	$S_4 \times S_3^2$	$S_3 \times S_4$ (144.183) $A_4 : S_3^2$ (432.747 and 432.748)	
	$S_4 \times (C_3^2 : C_4)$	$(C_3^2 \times A_4) : C_4$ (432.743)	
	$S_4 \times (C_2 \times S_4)$	$C_2 \times S_4$ (48.48) $C_2^3 : S_4$ (192.1538) S_4^2 (576.8653) $A_4^2 : C_2^2$ (576.8657)	
	$S_4 \times A_5$	None	
	$S_4 \times \text{SO}^+(4, 2)$	$C_6^2 : D_{12}$ (864.4669) $S_3^2 : S_4$ (864.4670)	
	$S_4 \times S_5$	$A_4 : S_5$ (1440.5847)	
	$S_4 \times A_6$	None	
	$S_4 \times S_6$	$A_4 : S_6$ (8640.o)	
(5, 5)	$C_5 \times C_5$	C_5 (5.1)	
	$C_5 \times D_5$	None	
	$C_5 \times F_5$	None	
	$C_5 \times A_5$	None	
	$C_5 \times S_5$	None	
	$D_5 \times D_5$	D_5 (10.1) $C_5 : D_5$ (50.4)	
	$D_5 \times F_5$	$C_5 : F_5$ (100.10)	

Continued on next page

Table A.1 - Continued from previous page

Factorisation	Product of Galois Groups	Subdirect (LMFDB ID)	Products
(5, 5)	$D_5 \times A_5$	None	
	$D_5 \times S_5$	$C_5 : S_5$ (600.145)	
	$F_5 \times F_5$	F_5 (20.3) $C_5 : F_5$ (100.11 and 100.12) $D_5 : F_5$ (200.42)	
	$F_5 \times A_5$	None	
	$F_5 \times S_5$	$A_5 : F_5$ (1200.939)	
	$A_5 \times A_5$	A_5 (60.5)	
	$A_5 \times S_5$	None	
	$S_5 \times S_5$	S_5 (120.34) $\text{PSO}^+(4, 5)$ (7200.d)	

Appendix B

Table of Transitive Subgroups That are Conjugate-Covered by Subgroups of Certain Indices

Table B.1: Transitive groups of certain degrees which can be conjugate-covered by subgroups of given indices

Factorisation	Group (LMFDB ID)
Degree 5	
(2, 3)	S_3 (6.1)
	D_6 (12.4)
Degree 6	
(2, 2, 2)	C_2^2 (4.2)
	C_2^3 (8.5)
Degree 7	
(2, 2, 3)	S_3 (6.1)
	D_6 (12.4)
	$C_2^2 \times S_3$ (24.14)
(2, 5)	D_5 (10.1)

Continued on next page

Table B.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)
(2, 5)	F_5 (20.3)
	D_{10} (20.4)
	$C_2 \times F_5$ (40.12)
(3, 4)	A_4 (12.3)
	S_4 (24.12)
	$C_2 \times A_4$ (24.13)
	$C_3 \times A_4$ (36.11)
	$C_2 \times S_4$ (48.48)
	$C_3 \times S_4$ (72.42)
	$C_3 : S_4$ (72.43)
	$S_3 \times A_4$ (72.44)
	$S_3 \times S_4$
	(144.183)
Degree 8	
(2, 2, 2, 2)	C_2^2 (4.2)
	C_2^3 (8.5)
	C_2^4 (16.14)
(2, 2, 4)	D_4 (8.3)
	$C_2 \times D_4$ (16.11)
	$C_2^2 \times D_4$ (32.46)
(2, 3, 3)	D_6 (12.4)
	$C_3 \times S_3$ (18.3)
	$C_3 : S_3$ (18.4)
	S_3^2 (36.10)
	$C_6 \times S_3$ (36.12)
	$C_6 : S_3$ (36.13)
	$S_3 \times D_6$ (72.46)
Degree 9	
(2, 2, 2, 3)	S_3 (6.1)
	D_6 (12.4)

Continued on next page

Table B.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)
(2, 2, 2, 3)	$C_2 \times C_6$ (12.5)
	$C_2 \times D_6$ (24.14)
	$C_2^2 \times C_6$ (24.15)
	$C_2^2 \times D_6$ (48.51)
(2, 2, 5)	D_5 (10.1)
	F_5 (20.3)
	D_{10} (20.4)
	$C_2 \times F_5$ (40.12)
	$C_2 \times D_{10}$ (40.13)
	$C_2^2 \times F_5$ (80.50)
(2, 3, 4)	$C_3 : C_4$ (12.1)
	D_6 (12.4)
	$C_4 \times S_3$ (24.5)
	D_{12} (24.6)
	$C_6 : C_4$ (24.7)
	$C_3 : D_4$ (24.8)
	S_4 (24.12)
	$C_2 \times A_4$ (24.13)
	$C_2 \times D_6$ (24.14)
	S_3^2 (36.10)
	$C_6 \times S_3$ (36.12)
	$C_4 \times D_6$ (48.35)
	$C_2 \times D_{12}$ (48.36)
	$S_3 \times D_4$ (48.38)
	$C_6 : D_4$ (48.43)
	$C_2 \times S_4$ (48.48)
	$C_2^2 \times A_4$ (48.49)
	$C_2^2 \times D_6$ (48.51)
	$C_3 \times S_4$ (72.42)
	$C_3 : S_4$ (72.43)
	$S_3 \times A_4$ (72.44)
	$S_3 \times D_6$ (72.46)
	$C_6 \times A_4$ (72.47)

Continued on next page

Table B.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)
(2, 3, 4)	$D_4 \times D_6$ (96.209)
	$C_2^2 \times S_4$ (96.226)
	$S_3 \times S_4$ (144.183)
	$C_6 \times S_4$ (144.188)
	$C_6 : S_4$ (144.189)
	$A_4 \times D_6$ (144.190)
	$D_6 \times S_4$ (288.1028)
	D_7 (14.1)
	F_7 (42.1)
	F_5 (20.3)
(4, 5)	$C_2 \times F_5$ (40.12)
	$C_4 \times F_5$ (80.30)
	$C_{20} : C_4$ (80.31)
	$D_{10} : C_4$ (80.34)
	$C_2^2 \times F_5$ (80.50)
	$D_4 \times F_5$ (160.207)
	$A_4 : F_5$ (240.192)
	$A_4 \times F_5$ (240.193)
	$F_5 \times S_4$ (480.1189)
Degree 10	
(2, 2, 2, 2, 2)	C_2^2 (4.2)
	C_2^3 (8.5)

Continued on next page

Table B.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)
(2, 2, 2, 2, 2)	C_2^4 (16.14)
	C_2^2 (4.2)
	$C_2 \times C_4$ (8.2)
	D_4 (8.3)
	C_2^3 (8.5)
	$C_2^2 \times C_4$ (16.10)
	$C_2 \times D_4$ (16.11)
	C_2^4 (16.14)
	$C_2^2 \times D_4$ (32.46)
	$C_2 \times S_4$ (48.48)
(2, 2, 2, 4)	$C_2^2 \times A_4$ (48.49)
	$C_2^2 \times S_4$ (96.226)
	S_3 (6.1)
	D_6 (12.4)
	$C_3 \times S_3$ (18.3)
	$C_3 : S_3$ (18.4)
	$C_2 \times D_6$ (24.14)
	S_3^2 (36.10)
	$C_6 \times S_3$ (36.12)
	$C_6 : S_3$ (36.13)
(2, 2, 3, 3)	$S_3 \times D_6$ (72.46)
	D_6 (12.4)
	$C_2 \times D_6$ (24.14)
	S_3^2 (36.10)
	$C_6 \times S_3$ (36.12)
	$C_2 \times S_4$ (48.48)
	$C_2^2 \times D_6$ (48.51)
	$\text{SO}^+(4, 2)$
	(72.40)
	$S_3 \times D_6$ (72.46)
(2, 2, 6)	$C_6 \times D_6$ (72.48)
	$C_2^2 \times S_4$ (96.226)

Continued on next page

Table B.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)
(2, 2, 2, 4)	$S_3^2 : C_2^2$ (144.186)
	D_6^2 (144.192)
	$C_2^3 \times S_4$ (192.1537)
	$C_6^2 : D_4$ (288.1031)
(2, 3, 5)	$C_5 \times S_3$ (30.1)
	$C_3 \times D_5$ (30.2)
	D_{15} (30.3)
	$C_3 \times F_5$ (60.6)
	$C_{15} : C_4$ (60.7)
	$S_3 \times D_5$ (60.8)
	$C_3 \times D_{10}$ (60.10)
	$S_3 \times C_{10}$ (60.11)
	D_{30} (60.12)
	$S_3 \times F_5$ (120.36)
	$C_6 \times F_5$ (120.40)
	$C_{30} : C_4$ (120.41)
	$S_3 \times D_{10}$ (120.42)
	$D_6 \times F_5$ (240.195)
	$C_3 : S_5$ (360.120)
	$S_3 \times A_5$ (360.121)
	$S_3 \times S_5$ (720.767)
	$C_6 : S_5$ (720.770)

Continued on next page

Table B.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)
(2, 3, 5)	$D_6 \times A_5$ (720.771)
	D_4 (8.3)
	$C_2^2 : C_4$ (16.3)
	$C_4 : C_4$ (16.4)
	$C_2 \times D_4$ (16.11)
	$C_2^3 : C_4$ (32.22)
	$C_4 \times D_4$ (32.25)
	$C_2^2 \wr C_2$ (32.27)
	$C_4 : D_4$ (32.28)
	and 32.34)
	$C_2^2 \times D_4$ (32.46)
	$C_2^3 : D_4$ (64.202)
	D_4^2 (64.226)
	$C_4 : S_4$ (96.187)
(2, 4, 4)	$\text{GL}(2, \mathbb{Z}/4)$ (96.195)
	$D_4 \times A_4$ (96.197)
	$D_4 \times S_4$ (192.1472)
	A_4 (12.3)
	S_4 (24.12)
	$C_2 \times A_4$ (24.13)
	S_3^2 (36.10)
	$C_3 \times A_4$ (36.11)
	$C_2 \times S_4$ (48.48)
	$C_2^2 \times A_4$ (48.49)
	$C_6.D_6$ (72.21)
	$C_3 : D_{12}$ (72.23)
	$C_3 \times S_4$ (72.42)
	$C_3 : S_4$ (72.43)
	$S_3 \times A_4$ (72.44)
(3, 3, 4)	

Continued on next page

Table B.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)
(3, 3, 4)	$S_3 : D_6$ (72.46)
	$C_2^2 \times S_4$ (96.226)
	$C_3 \times S_3^2$ (108.38)
	$C_3 : S_3^2$ (108.40)
	$D_6 : D_6$
	(144.154)
	$S_3 \times S_4$
	(144.183)
(2, 2, 2, 4)	S_3^3 (216.162)
	$C_7 : C_3$ (21.1)
	F_7 (42.1)
	$C_{21} : C_3$ (63.3)
	$C_3 \times F_7$ (126.7)
	$C_{21} : C_6$ (126.8)
	$C_{21} : C_6$ (126.9)
	$S_3 \times F_7$ (252.26)
(4, 6)	A_4 (12.3)
	S_4 (24.12)
	$C_2 \times A_4$ (24.13)
	$C_3 \times A_4$ (36.11)
	$A_4 : C_4$ (48.30)
	$C_4 \times A_4$ (48.31)
	$C_2 \times S_4$ (48.48)
	$C_2^2 \times A_4$ (48.49)
	$C_2^2 : A_4$ (48.50)
	$C_3 \times S_4$ (72.42)
	$C_3 : S_4$ (72.43)
	$S_3 \times A_4$ (72.44)
	$C_6 \times A_4$ (72.47)
	$C_4 \times S_4$ (96.186)
	$C_4 : S_4$ (96.187)
	$C_2^2.S_4$ (96.194)

Continued on next page

Table B.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)
(4, 6)	$\mathrm{GL}(2, \mathbb{Z}/4)$
	(96.195)
	$C_2^3 : C_{12}$
	(96.196)
	$D_4 \times A_4$
	(96.197)
	$C_2^2 \times S_4$ (96.226)
	$C_2^2 : S_4$ (96.227)
	$C_2^3 \times A_4$
	(96.228)
	$C_2^3 : A_4$ (96.229)
	$S_3 \times S_4$
	(144.183)
	A_4^2 (144.184)
	$C_6 \times S_4$
	(144.188)
	$C_6 : S_4$
	(144.189)
	$A_4 \times D_6$
	(144.190)
	$C_2^4.D_6$
	(192.1469)
	$C_2^3 : D_{12}$
	(192.1470)
	$D_4 \times S_4$
	(192.1472)
	$C_2 \times \mathrm{GL}(2, \mathbb{Z}/4)$
	(192.1488)
	$C_2^5 : C_6$
	(192.1497)
	$C_2^3 \times S_4$
	(192.1537)

Continued on next page

Table B.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)
(4, 6)	$C_2^3 : S_4$ (192.1538)
	$C_3^2 : S_4$ (216.164)
	$C_6^2 : C_6$ (216.166)
	$A_4 \times S_4$ (288.1024)
	$\text{PSO}^+(4, 3)$ (288.1026)
	$D_6 \times S_4$ (288.1028)
	$C_2 \times A_4^2$ (288.1029)
	$(C_3^2 \times A_4) : C_4$ (432.743)
	$C_6^2 : C_{12}$ (432.744)
	$C_6^2 : D_6$ (432.745)
	$A_4 : S_3^2$ (432.747 and 432.748)
	$A_4 \times S_3^2$ (432.749)
	S_4^2 (576.8653)
	$A_4^2 : C_2^2$ (576.8655)
	$A_4^2 : C_2^2$ (576.8657)
	$A_4 \times A_5$ (720.768)
	$(C_3^2 : C_4) \times S_4$ (864.4668)

Continued on next page

Table B.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)
(4, 6)	$C_6^2 : D_{12}$ (864.4669)
	$S_3^2 : S_4$ (864.4670)
	$D_6^2 : C_6$ (864.4671)
	$S_4 \times S_3^2$ (864.4673)
	$C_2 \times S_4^2$ (1152.157851)
	$A_4 \times S_5$ (1440.5846)
	$A_4 : S_5$ (1440.5847)
	$S_4 \times A_5$ (1440.5848)
	$D_6^2 : D_6$ (1728.47847)
	$S_4 \times S_5$ (2880.dv)
	$A_4 \times A_6$ (4320.bh)
	$A_4 \times S_6$ (8640.n)
	$A_4 : S_6$ (8640.o)
	$S_4 \times A_6$ (8640.p)

Appendix C

Table of Possible Galois Groups of Strongly Intersective Polynomials

Table C.1: Possible Galois groups of strongly intersective polynomials of degrees 5 to 10, with some examples

Factorisation	Galois Group (LMFDB ID)	Example Strongly Intersective Polynomial
Degree 5		
(2, 3)	S_3 (6.1)	$(x^3 - 19)(x^2 + x + 1)$
Degree 6		
(2, 2, 2)	C_2^2 (4.2)	$(x^2 - 2)(x^2 - 17)(x^2 - 34)$
Degree 7		
(2, 2, 3)	S_3 (6.1)	$(x^3 - 19)(x^2 + x + 1)(x^2 + 3)$
	D_6 (12.4)	$(x^3 - 73)(x^2 + x + 1)(x^2 - 5)$
(2, 5)	D_5 (10.1)	$(x^5 - 2x^4 + 3x^3 - 3x^2 + x + 1)(x^2 + 103)$
	F_5 (20.3)	$(x^5 - x^4 + x^2 + 3x + 1)(x^2 - 17)$
(3, 4)	A_4 (12.3)	$(x^4 - x^3 - 3x + 4)(x^3 - x^2 - 4x - 1)$
	S_4 (24.12)	$(x^4 - x + 1)(x^3 - 4x - 1)$
	$C_3 : S_4$ (72.43)	—

Continued on next page

Table C.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)	Example Strongly Intersective Polynomial
Degree 8		
(2, 2, 2, 2)	C_2^2 (4.2)	$(x^2 - 2)(x^2 - 17)(x^2 - 34)(x^2 - 68)$
	C_2^3 (8.5)	$(x^2 - 2)(x^2 - 13)(x^2 - 17)(x^2 - 221)$
(2, 2, 4)	D_4 (8.3)	$(x^4 + x^2 - 2x + 1)(x^2 - x - 4)(x^2 + 1)$
	$C_2 \times D_4$ (16.11)	$(x^4 - x^3 - x^2 + x + 1)(x^2 - x + 1)$ $(x^2 - x - 15)$
(2, 3, 3)	D_6 (12.4)	$(x^3 + 2)(x^3 - 2)(x^2 - x + 6)$
	$C_3 \times S_3$ (18.3)	$(x^3 - x^2 + 1)(x^3 - x^2 - 4x - 1)(x^2 - x + 6)$
	$C_3 : S_3$ (18.4)	—
	S_3^2 (36.10)	$(x^3 - x^2 + 1)(x^3 + x - 1)(x^2 - x + 6)$
	$C_6 : S_3$ (36.13)	$(x^3 - x^2 - 3x - 3)(x^3 - x^2 + 6x - 12)$ $(x^2 - x + 3)$
Degree 9		
(2, 2, 2, 3)	S_3 (6.1)	$(x^3 - 19)(x^2 + x + 1)(x^2 + 3)(x^2 - x + 1)$
	D_6 (12.4)	$(x^3 - 73)(x^2 + x + 1)(x^2 - 5)(x^2 + 3)$
	$C_2 \times C_6$ (12.5)	$(x^3 - 3x - 1)(x^2 - x + 3)(x^2 + 11)$ $(x^2 - x - 1)$
	$C_2 \times D_6$ (24.14)	$(x^3 - 3)(x^2 - x + 3)(x^2 + 11)(x^2 - x - 1)$
(2, 2, 5)	D_5 (10.1)	$(x^5 - 2x^4 + 2x^3 - x^2 + 1)(x^2 - x + 12)$ $(x^2 + 47)$
	F_5 (20.3)	$(x^5 - x^4 + x^2 + 3x + 1)(x^2 - x - 4)(x^2 - 17)$
	D_{10} (20.4)	$(x^5 - x^4 + x^3 - 2x^2 + 3x - 1)(x^2 - 79)$ $(x^2 - x + 20)$
	$C_2 \times F_5$ (40.12)	$(x^5 - x^4 + x^2 + 3x + 1)(x^2 - x - 4)(x^2 - 2)$
(2, 3, 4)	$C_3 : C_4$ (12.1)	$(x^4 - x^3 - 663x^2 + 1981x + 13363)$ $(x^3 - x^2 - 121x + 246)(x^2 - x - 7)$
	D_6 (12.4)	$(x^4 - x^3 - 5x^2 - 6x + 36)(x^3 - x^2 + 1)$ $(x^2 - x + 6)$
	$C_4 \times S_3$ (24.5)	$(x^4 - x^3 - 15x^2 - 18x - 4)(x^3 - 30x - 44)$ $(x^2 - 43)$
	D_{12} (24.6)	—

Continued on next page

Table C.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)	Example Strongly Intersective Polynomial
(2, 3, 4)	$C_6 : C_4$ (24.7)	—
	$C_3 : D_4$ (24.8)	$(x^4 - x^3 + 8x^2 - 2x + 13)(x^3 - 4x - 1)$ $(x^2 - x - 57)$
	S_4 (24.12)	$(x^4 - x + 1)(x^3 - 4x - 1)$ $(x^2 - x - 57)$
	$C_2 \times A_4$ (24.13)	—
	$C_2 \times D_6$ (24.14)	$(x^4 - x^3 + 5x^2 + 2x + 4)(x^3 - x^2 + 1)$ $(x^2 - x + 2)$
	$C_2 \times D_{12}$ (48.36)	—
	$S_3 \times D_4$ (48.38)	$(x^4 - x^3 - 3x^2 - x + 1)(x^3 - x^2 + 1)$ $(x^2 - x + 6)$
	$C_6 : D_4$ (48.43)	$(x^4 - 2x^3 + 3x^2 - 2x - 1)(x^3 - x^2 + 1)$ $(x^2 - x + 2)$
	$C_2 \times S_4$ (48.48)	$(x^4 - x + 1)(x^3 - 4x - 1)(x^2 - x + 6)$
	$C_3 \times S_4$ (72.42)	—
	$C_3 : S_4$ (72.43)	—
	$S_3 \times A_4$ (72.44)	—
	$S_3 \times S_4$ (144.183)	—
	$C_6 : S_4$ (144.189)	—
(2, 7)	D_7 (14.1)	$(x^7 - x^6 - x^5 + x^4 - x^3 - x^2 + 2x + 1)$ $(x^2 + 71)$
	F_7 (42.1)	$(x^7 - 2x^6 - 2x^5 + x^4 + 6x^3 - x - 4)(x^2 + 11)$
(4, 5)	F_5 (20.3)	$(x^5 - 2x^4 + 7x^3 - 4x^2 + 11x + 6)$ $(x^4 - x^3 + 13x^2 - 19x + 361)$
	$C_2 \times F_5$ (40.12)	$(x^5 - x^4 + x^2 + 3x + 1)$ $(x^4 - x^3 - 6x^2 + x + 1)$ and $(x^5 - x^4 + x^2 + 3x + 1)$ $(x^4 - x^3 + 5x^2 + 4x + 16)$
	$C_{20} : C_4$ (80.31)	—
	$D_{10} : C_4$ (80.34)	—

Continued on next page

Table C.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)	Example Strongly Intersective Polynomial
(4, 5)	$A_4 : F_5$ (240.192)	—
Degree 10		
(2, 2, 2, 2, 2)	C_2^2 (4.2)	$(x^2 - 2)(x^2 - 17)(x^2 - 34)(x^2 - 68)$ $(x^2 - 153)$
	C_2^3 (8.5)	$(x^2 - 2)(x^2 - 17)(x^2 - 34)(x^2 - 68)$ $(x^2 - 102)$
	C_2^4 (16.14)	$(x^2 - 15)(x^2 - 17)(x^2 - 557)(x^2 - 255)$ $(x^2 - 871711)$
(2, 2, 2, 4)	C_2^2 (4.2)	$(x^4 - 240x^2 + 7396)(x^2 - 103)(x^2 - 17)$ $(x^2 - 1751)$
	$C_2 \times C_4$ (8.2)	$(x^4 - x^3 + 2x^2 + 4x + 3)(x^2 - 13)(x^2 - 117)$ $(x^2 - 17)$
	D_4 (8.3)	$(x^4 - x^3 - x^2 + x + 1)(x^2 + 3)(x^2 - 13)$ $(x^2 + 39)$
	C_2^3 (8.5)	$(x^4 + 43x^2 + 900)(x^2 - 17)(x^2 - 103)$ $(x^2 - 1751)$
	$C_2^2 \times C_4$ (16.10)	$(x^4 - x^3 + 2x^2 + 4x + 3)(x^2 - 13)(x^2 - 53)$ $(x^2 - 17)$
	$C_2 \times D_4$ (16.11)	$(x^4 + x^2 - 2x + 1)(x^2 - x - 4)(x^2 - 2)$ $(x^2 - 17)$
	C_2^4 (16.14)	$(x^4 - x^3 + 2x^2 + x + 1)(x^2 - x + 5)$ $(x^2 - x + 3)(x^2 - x - 1)$
	$C_2^2 \times D_4$ (32.46)	$(x^4 + x^2 - 2x + 1)(x^2 - x - 4)(x^2 - 2)$ $(x^2 - 13)$
	$C_2 \times S_4$ (48.48)	—
	$C_2^2 \times A_4$ (48.49)	—
	$C_2^2 \times S_4$ (96.226)	—
(2, 2, 3, 3)	S_3 (6.1)	$(x^3 - x - 1)(x^3 - 3x^2 + 2x - 1)(x^2 + 5)$ $(x^2 - x + 6)$
	D_6 (12.4)	$(x^3 - x - 1)(x^3 - 3x^2 + 2x - 1)(x^2 + 5)$ $(x^2 - x + 6)$

Continued on next page

Table C.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)	Example Strongly Intersective Polynomial
(2, 2, 3, 3)	$C_3 \times S_3$ (18.3)	$(x^3 + x - 1)(x^3 - x^2 - 2x + 1)(x^2 - x + 8)$ $(x^2 + 31)$
	$C_3 : S_3$ (18.4)	—
	$C_2 \times D_6$ (24.14)	—
	S_3^2 (36.10)	—
	$C_6 \times S_3$ (36.12)	—
	$C_6 : S_3$ (36.13)	—
	$S_3 \times D_6$ (72.46)	—
(2, 2, 6)	D_6 (12.4)	—
	$C_2 \times D_6$ (24.14)	—
	S_3^2 (36.10)	—
	$C_6 \times S_3$ (36.12)	—
	$C_2 \times S_4$ (48.48)	—
	$SO^+(4, 2)$ (72.40)	—
	$S_3 \times D_6$ (72.46)	—
	$C_2^2 \times S_4$ (96.226)	—
	$S_3^2 : C_2^2$ (144.186)	—
(2, 3, 5)	$C_5 \times S_3$ (30.1)	—
	$C_3 \times D_5$ (30.2)	—
	D_{15} (30.3)	—
	$C_{15} : C_4$ (60.7)	—
	$S_3 \times D_5$ (60.8)	—
	D_{30} (60.12)	—
	$S_3 \times F_5$ (120.36)	—
	$C_{30} : C_4$ (120.41)	—
	$C_3 : S_5$ (360.120)	—
	$S_3 \times A_5$ (360.121)	—

Continued on next page

Table C.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)	Example Strongly Intersective Polynomial
(2, 3, 5)	$S_3 \times S_5$ (720.767)	—
	$C_6 : S_5$ (720.770)	—
(2, 4, 4)	D_4 (8.3)	—
	$C_2^2 : C_4$ (16.3)	—
	$C_4 : C_4$ (16.4)	—
	$C_2 \times D_4$ (16.11)	—
	$C_2^3 : C_4$ (32.22)	—
	$C_4 \times D_4$ (32.25)	—
	$C_2^2 \wr C_2$ (32.27)	—
	$C_4 : D_4$ (32.28 and 32.34)	—
	$C_2^2 \times D_4$ (32.46)	—
	$C_2^3 : D_4$ (64.202)	—
	D_4^2 (64.226)	—
	$C_4 : S_4$ (96.187)	—
	$\text{GL}(2, \mathbb{Z}/4)$ (96.195)	—
	$D_4 \times A_4$ (96.197)	—
	$D_4 \times S_4$ (192.1472)	—
(3, 3, 4)	A_4 (12.3)	—
	S_4 (24.12)	—
	S_3^2 (36.10)	—
	$C_3 \times A_4$ (36.11)	—
	$C_6.D_6$ (72.21)	—
	$C_3 : D_{12}$ (72.23)	—
	$C_3 \times S_4$ (72.42)	—
	$C_3 : S_4$ (72.43)	—
	$S_3 \times A_4$ (72.44)	—
	$S_3 : D_6$ (72.46)	—

Continued on next page

Table C.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)	Example Strongly Intersective Polynomial
(3, 3, 4)	$D_6 : D_6$ (144.154)	—
	$S_3 \times S_4$ (144.183)	—
(3, 7)	$C_7 : C_3$ (21.1)	$(x^7 - x^6 - 15x^5 + 20x^4 + 33x^3 - 22x^2 - 32x - 8)$ $(x^3 - x^2 - 104x - 371)$
	F_7 (42.1)	$(x^7 - 3x^6 + 3x^5 - 3x^4 + 3x^3 - 3x^2 + 10x - 9)$ $(x^3 - 21x - 28)$
	$C_{21} : C_6$ (126.9)	—
	A_4 (12.3)	$(x^6 - 3x^4 - 10x^3 - 18x^2 - 18x - 9)$ $(x^4 - x^3 + 3x^2 + x + 20)$
(4, 6)	S_4 (24.12)	$(x^6 - x^5 - x^4 + x^3 - x^2 - x + 1)$ $(x^4 + x^2 - x + 1)$ and $(x^6 - x^4 - x^3 - x^2 + 1)(x^4 - x + 1)$
	$C_2 \times A_4$ (24.13)	$(x^6 - 2x^5 + 2x^4 - 3x^3 + 2x^2 - 2x + 1)$ $(x^4 - x^3 + 5x^2 - 4x + 3)$
	$A_4 : C_4$ (48.30)	—
	$C_4 \times A_4$ (48.31)	—
	$C_2 \times S_4$ (48.48)	—
	$C_2^2 \times A_4$ (48.49)	—
	$C_2^2 : A_4$ (48.50)	—
	$C_3 \times S_4$ (72.42)	—
	$C_3 : S_4$ (72.43)	—
	$S_3 \times A_4$ (72.44)	—
	$C_4 \times S_4$ (96.186)	—
	$C_4 : S_4$ (96.187)	—
	$C_2^2.S_4$ (96.194)	—
	$\text{GL}(2, \mathbb{Z}/4)$ (96.195)	—

Continued on next page

Table C.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)	Example Strongly Intersective Polynomial
(4, 6)	$D_4 \times A_4$ (96.197)	—
	$C_2^2 \times S_4$ (96.226)	—
	$C_2^2 : S_4$ (96.227)	—
	$C_2^3 : A_4$ (96.229)	—
	$S_3 \times S_4$ (144.183)	—
	$C_6 : S_4$ (144.189)	—
	$C_2^3 : D_{12}$ (192.1470)	—
	$D_4 \times S_4$ (192.1472)	—
	$C_2 \times \text{GL}(2, \mathbb{Z}/4)$ (192.1488)	—
	$C_2^3 : S_4$ (192.1538)	—
	$C_3^2 : S_4$ (216.164)	—
	$A_4 \times S_4$ (288.1024)	—
	$\text{PSO}^+(4, 3)$ (288.1026)	—
	$(C_3^2 \times A_4) : C_4$ (432.743)	—
	$A_4 : S_3^2$ (432.747 and 432.748)	—
	S_4^2 (576.8653)	—
	$A_4^2 : C_2^2$ (576.8657)	—
	$C_6^2 : D_{12}$ (864.4669)	—

Continued on next page

Table C.1 - Continued from previous page

Factorisation	Galois Group (LMFDB ID)	Example Strongly Intersective Polynomial
(4, 6)	$S_3^2 : S_4$ (864.4670)	—
	$A_4 : S_5$ (1440.5847)	—
	$A_4 : S_6$ (8640.o)	—

Appendix D

Background

This Chapter contains preliminaries and background information relevant to the main body of the thesis. Section [D.1](#) covers basic algebraic number theory, including ramification, inertia degrees, and the definition of decomposition groups, but excluding discriminants. Section [D.2](#) contains information on discriminants of ring extensions, of which the discriminant of a number field is a special case. Section [D.3](#) describes Frobenius elements of Galois number fields, ending with some brief exposition on the Chebotarev Density Theorem. Section [D.4](#) is the most self-contained and introduces the p -adic integers $\mathbb{Z}_p$ and the p -adic numbers $\mathbb{Q}_p$, as well as a general treatment of discrete absolute values which applies to finite extensions of $\mathbb{Q}_p$. Section [D.5](#) describes finite extensions of $\mathbb{Q}_p$, including the definitions of ramification and inertia degrees. Finally, Section [D.6](#) explains how the p -adic absolute value can be extended to both number fields and finite extensions of $\mathbb{Q}_p$.

D.1 Algebraic Number Theory

This section aims to introduce ramification degrees and inertia degrees, as well as their relation to discriminants, which are fundamental quantities associated with field extensions of $\mathbb{Q}$.

We assume familiarity with the theory of finite fields, field extensions, and Galois theory of finite extensions, as well as basic commutative algebra. As we omit the proofs, references will be given where possible, with most coming from the textbooks by Marcus ([\[46, Chapters 2 and 3\]](#)) and Neukirch ([\[52, Chapter I\]](#)).

It is possible for two non-isomorphic extensions of $\mathbb{Q}$, e.g., $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$, to have isomorphic Galois groups. The numerical invariants mentioned above will provide finer

distinctions between such extensions. It may be helpful to think of the Galois group as the “algebraic” information contained in the extension, while the invariants from this section can be thought of as “arithmetic” information.

Definition D.1.1. A **number field** is a field extension $L/\mathbb{Q}$ of the rational numbers of finite degree.

Note that by general field theory, specifically the *Primitive Element Theorem*, any number field can be written as a simple field extension $\mathbb{Q}(\theta)$ for some algebraic number $\theta \in \mathbb{C}$, i.e., a complex number for which there exists a polynomial $f(x) \in \mathbb{Q}[x]$ with $f(\theta) = 0$. This also implies the existence of a unique polynomial $m_\theta(x) \in \mathbb{Q}[x]$ of minimal degree which is irreducible such that $m_\theta(\theta) = 0$. In fact, if $n = \deg(m_\theta)$, then $\mathbb{Q}(\theta)$ will have degree n over $\mathbb{Q}$ and can be constructed as $\{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} : a_i \in \mathbb{Q}\}$.

Example D.1.1. $\mathbb{Q}(\sqrt{2}) := \{a_0 + a_1\sqrt{2} : a_i \in \mathbb{Q}\}$ and $\mathbb{Q}(\sqrt[3]{2}) := \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2\}$ are number fields with degrees 2 and 3 over $\mathbb{Q}$, respectively.

By inspecting a proof of the *Primitive Element Theorem* ([23, Theorem 25 Chapter 14]), the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, which we define as the minimal subfield of $\mathbb{C}$ containing $\mathbb{Q}$, $\sqrt{2}$, and $\sqrt{3}$, can be rewritten as $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.

More abstractly, let $f(x) := x^3 - x^2 - 2x - 8$, which is irreducible over $\mathbb{Q}$, and let θ be a root of f . Then $\mathbb{Q}(\theta)$ is a **cubic field**, i.e., a number field of degree 3. This particular cubic field is rather infamous and is sometimes called **Dedekind’s cubic field**; see Conrad’s expository notes ([22]).

We wish to mimic the relationship between $\mathbb{Q}$ and its distinguished subring $\mathbb{Z}$ for an arbitrary number field. One possibility is to notice that, for example, the rational number $\frac{1}{2}$ is a root of $2x - 1 \in \mathbb{Z}[x]$, but it is *not* the root of any *monic* polynomial with integer coefficients - we always need a leading coefficient to clear denominators. This connection may feel tenuous, but works surprisingly well in general:

Definition D.1.2. Let $L/\mathbb{Q}$ be a number field. The set

$$\mathcal{O}_L := \{\alpha \in L : \text{there exists a monic polynomial } f(x) \in \mathbb{Z}[x] \text{ such that } f(\alpha) = 0\}$$

is called the **ring of (algebraic) integers of L** .

Example D.1.2. The ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$ i.e., $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ ([46, Chapter 2, Corollary 1]).

The following fact can be proved with several methods, including the theory of symmetric polynomials and the theory of finitely generated modules over PIDs:

Proposition D.1.1. [46, Chapter 2, Corollary 1 and remarks preceding Theorem 9] *Let $L/\mathbb{Q}$ be a number field and $n := [L : \mathbb{Q}]$. Then the ring of integers $\mathcal{O}_L$ is a subring of L , and therefore is an integral domain. In fact, L is the field of fractions of $\mathcal{O}_L$. Moreover, $\mathcal{O}_L$ is a free $\mathbb{Z}$ -module of rank n .*

The last sentence in Proposition D.1.1 means that there are $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$ such that, as $\mathbb{Z}$ -modules,

$$\mathcal{O}_L \cong \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n.$$

Note that it would've been completely equivalent to start with a ring A which is also a free $\mathbb{Z}$ -module of finite rank, n , and then define a number field to be the field of fractions of A . As a consequence, this field would be a finite extension of $\mathbb{Q}$ of degree n .

Example D.1.3. *Let $L := \mathbb{Q}(i)$, which is a number field of degree 2. Then one can show that $\mathcal{O}_L = \mathbb{Z}[i] := \{a_0 + a_1i : a_j \in \mathbb{Z}\}$; in particular, a basis of $\mathcal{O}_L$ as a $\mathbb{Z}$ -module is $\{1, i\}$. The ring $\mathbb{Z}[i]$ is called the **Gaussian integers**, and $\mathbb{Q}(i)$ is called the **Gaussian numbers**.*

For $L' := \mathbb{Q}(\sqrt{5})$. One might expect that $\mathcal{O}_{L'} = \mathbb{Z}[\sqrt{5}]$, similarly to the above... which is wrong! In fact,

$$\mathcal{O}_{L'} = \mathbb{Z} \left[\frac{1 + \sqrt{5}}{2} \right].$$

The fact that L' contains “integers” with denominators stems from the fact that $5 \equiv 1 \pmod{4}$. Interestingly, this congruence condition modulo 4 exactly distinguishes these two cases, and further, every number field of degree 2 is captured by these two cases.

In both prior examples, we obtained the ring of integers of a number field by adjoining a single element of $\mathbb{Z}$. This trend does not continue past degree 2: Let $L'' = \mathbb{Q}(\theta)$ be Dedekind's cubic field from Example D.1.1. Then one can show that

$$\mathcal{O}_{L''} = \mathbb{Z} \left[\theta, \frac{4}{\theta} \right],$$

*and further, that $\mathcal{O}_{L''}$ cannot be obtained by adjoining a single algebraic number to $\mathbb{Z}$ ([22, Theorem 1.1 and Corollary 1.2]). This type of number field is called **non-monogenic**. The existence of non-monogenic fields is responsible for many computational difficulties in algebraic number theory.*

Historically, number fields were introduced to study questions about prime factorisation, and we will follow suit.

Definition D.1.3. A **rational prime** is a prime number in $\mathbb{Z}$. More generally, if $L/\mathbb{Q}$ is a number field, then a **prime of L** means a non-zero prime ideal of the ring of integers $\mathcal{O}_L$.

A lot can be learned about rational primes using the primes of a given number field. We begin to solidify the relationship now.

Definition D.1.4. Let $L/\mathbb{Q}$ be a number field, and $\mathfrak{p}$ be a prime of L . If $p \in \mathbb{Z}$ is a rational prime such that $p\mathcal{O}_L \subseteq \mathfrak{p}$, then we say that $\mathfrak{p}$ **lies above** p and that p **lies below** $\mathfrak{p}$.

Example D.1.4. In the Gaussian numbers $L := \mathbb{Q}(i)$ with its ring of integers $\mathcal{O}_L = \mathbb{Z}[i]$, the ideal $3\mathcal{O}_L$ is prime, but $13\mathcal{O}_L$ is not. In fact, there are two primes of L lying above $13\mathcal{O}_L$ (made precise in Proposition D.1.3), namely, $\langle 2+3i \rangle$ and $\langle 2-3i \rangle$. A third behaviour is demonstrated by $2\mathcal{O}_L$, which has one prime lying above it with “multiplicity” two - more in Definition D.1.5.

The next pair of results clarifies the relationship between primes of $\mathbb{Z}$ and primes of $\mathcal{O}_L$.

Proposition D.1.2. [46, Chapter 3, Theorems 19 and 20] Let $L/\mathbb{Q}$ be a number field, and $\mathfrak{p}$ be a prime of L . Then there is a unique rational prime p such that $\mathfrak{p}$ lies above p , and in fact, $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$.

Proposition D.1.3. [46, Chapter 3, Theorems 14 and 16] Let $L/\mathbb{Q}$ be a number field. Then $\mathcal{O}_L$ is a Dedekind domain, i.e., every ideal I of $\mathcal{O}_L$ factors uniquely as a product of prime ideals of $\mathcal{O}_L$. In particular, if p is a rational prime, then the primes of L lying above p are the ideals appearing in the factorisation of $p\mathcal{O}_L$.

Example D.1.5. Continuing Example D.1.4 where $L = \mathbb{Q}(i)$ and $\mathcal{O}_L = \mathbb{Z}[i]$, with some effort, one can show that

$$13\mathcal{O}_L = \langle 2+3i \rangle \langle 2-3i \rangle$$

and

$$2\mathcal{O}_L = \langle 1+i \rangle^2,$$

and that $\langle 2+3i \rangle$, $\langle 2-3i \rangle$, and $\langle 1+i \rangle$ are prime in $\mathbb{Z}[i]$.

Example D.1.6. Let θ be a root of the irreducible cubic $f(x) := x^3 - 3x - 1 \in \mathbb{Q}[x]$, and let $L = \mathbb{Q}(\theta)$, which is of degree 3. One can show that $\mathcal{O}_L = \mathbb{Z}[\theta]$, and that we have the prime ideal factorisation

$$3\mathcal{O}_L = \langle 3, \theta + 2 \rangle^3.$$

On the other hand, both $2\mathcal{O}_L$ and $5\mathcal{O}_L$ remain prime in $\mathcal{O}_L$.

The seemingly innocuous fact that $2\mathcal{O}_L = \langle 1 + i \rangle^2$ in Example D.1.5, and $3\mathcal{O}_L = \langle 3, \theta + 2 \rangle^3$ in Example D.1.6, have repeated prime ideal factors carries extremely important information about the respective number fields.

Definition D.1.5. Let $L/\mathbb{Q}$ be a number field, and p a rational prime. By Proposition D.1.3, there exist primes $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ of L such that

$$p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

where $e_i \in \mathbb{Z}_{>0}$. The e_i are called the **ramification degrees** or **ramification indices** of $\mathfrak{p}_i$ over p in L . When we wish to emphasise the dependence on L , $\mathfrak{p}_i$, and p , we may write e_i as $e_L(\mathfrak{p}_i | p)$ or $e(\mathfrak{p}_i | p)$. If $e_i > 1$ for any i , then we say that p **ramifies** or **is ramified** in L ; we may also say that L **ramifies** or **is ramified at** p . Otherwise, we say that p is **unramified** in L and that L is **unramified at** p .

Example D.1.7. Continuing Example D.1.6, we see that $L = \mathbb{Q}(\theta)$ is unramified at 2 and 5 and ramified at 3. Notice also that the ramification degrees appear to be bounded by $3 = [L : \mathbb{Q}]$, which was also the case in D.1.5, where 2 is ramified.

If $L/\mathbb{Q}$ is a number field and p is a rational prime with factorisation $p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ in $\mathcal{O}_L$, then by the Chinese Remainder Theorem,

$$\mathcal{O}_L/p\mathcal{O}_L \cong (\mathcal{O}_L/\mathfrak{p}_1^{e_1}) \times \cdots \times (\mathcal{O}_L/\mathfrak{p}_g^{e_g}).$$

Now if some $e_i > 1$, then the residue class of any element of $\mathfrak{p}_i \setminus \mathfrak{p}_i^{e_i}$ is a non-zero nilpotent of $\mathcal{O}_L/\mathfrak{p}_i^{e_i}$, hence $\mathcal{O}_L/p\mathcal{O}_L$ has a non-zero nilpotent. Thus, we can relate ramification to the algebraic structure of a quotient of $\mathcal{O}_L$: p ramifies in $L/\mathbb{Q}$ precisely when $\mathcal{O}_L/p\mathcal{O}_L$ has a non-zero nilpotent element.

In general, unramified primes in a fixed number field $L/\mathbb{Q}$ come in infinite families which behave similarly to each other. In contrast, primes that ramify in L may behave drastically differently from each other. Fortunately, it turns out that L can only be ramified at a finite number of rational primes, a proof of which requires the **discriminant**. We simply state the result here, with the explanation being left to Section D.2:

Proposition D.1.4. [46, Chapter 3, Theorem 24 and Chapter 4, Theorem 34][18, Theorem 1.3] Let $L/\mathbb{Q}$ be a number field. There is a non-zero integer associated with $L/\mathbb{Q}$, called the **discriminant of L** and denoted by $\text{disc}(L)$, such that a rational prime p ramifies in L if and only if $p \mid \text{disc}(L)$. In particular, a given number field has only finitely many ramified rational primes.

Example D.1.8. By Example D.2.5, $\text{disc}(\mathbb{Q}(i)) = -2^2$, so the only ramified rational prime in the Gaussian numbers is 2. Indeed, the factorisation

$$2\mathbb{Z}[i] = \langle 1 + i \rangle^2$$

confirms that 2 ramifies.

We also saw in Example D.2.5 that $\text{disc}(\mathbb{Q}(\sqrt[3]{-23})) = -3^2 \cdot 23^2$, so 3 and 23 are the only ramified primes in this cubic field. In fact, one can find primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ such that

$$3\mathbb{Z}[\sqrt[3]{-23}] = \mathfrak{p}_1^3$$

and

$$23\mathbb{Z}[\sqrt[3]{-23}] = \mathfrak{p}_2^3.$$

In Dedekind's cubic $\mathbb{Q}(\theta)$, where θ is a root of $f(x) := x^3 - x^2 - 2x - 8$ - which has ring of integers $\mathbb{Z}[\theta, \frac{4}{\theta}]$ - one can show that $\text{disc}(\mathbb{Q}(\theta)) = -503$, and there are primes $\mathfrak{p}_3$ and $\mathfrak{p}_4$ such that

$$503\mathbb{Z}\left[\theta, \frac{4}{\theta}\right] = \mathfrak{p}_3\mathfrak{p}_4^2.$$

From the examples, one might conjecture that the ramification degree is always bounded above by the degree of the number field. This is true, but the following important quantities will lead to a more refined constraint:

Proposition D.1.5. [46, Chapter 3, Theorem 14 and remarks after Theorem 20] Let $L/\mathbb{Q}$ be a number field, and $\mathfrak{p}$ a prime of L . Then $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}_L$, so that $\mathcal{O}_L/\mathfrak{p}$ is a field. In fact, $\mathcal{O}_L/\mathfrak{p}$ is a finite field, and if p is the rational prime lying below $\mathfrak{p}$, then $\mathcal{O}_L/\mathfrak{p}$ is an extension of $\mathbb{F}_p$.

The proof that $\mathcal{O}_L/\mathfrak{p}$ is a field is interesting in its own right: By primality this quotient is an integral domain, but one can show that it is finite, and a finite integral domain is always a field.

The degree of the extension $[\mathcal{O}_L/\mathfrak{p} : \mathbb{F}_p]$, together with the ramification degree $e(\mathfrak{p} \mid p)$, provides essential information about factorisations of p .

Definition D.1.6. Let $L/\mathbb{Q}$ be a number field, p a rational prime, and $\mathfrak{p}$ a prime of L lying above p . The finite field $\mathcal{O}_L/\mathfrak{p}$ is called the **residue field of L with respect to $\mathfrak{p}$** , or simply the **residue field of L** depending on context. The degree of the extension $(\mathcal{O}_L/\mathfrak{p})/\mathbb{F}_p$ of finite fields is called the **residue class degree** or **inertia degree of $\mathfrak{p}$ over p** .

When considering prime ideal factorisations, i.e., when we write the ideal $p\mathcal{O}_L$ as

$$p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

the inertia degree $(\mathcal{O}_L/\mathfrak{p}_i)/\mathbb{F}_p$ is denoted by f_i , or possibly $f_L(\mathfrak{p}_i \mid p)$ or $f(\mathfrak{p}_i \mid p)$, to emphasise the relationship between $\mathfrak{p}_i$ and p .

Example D.1.9. In $\mathbb{Q}(i)$, whose ring of integers is $\mathbb{Z}[i]$, one can show without too much effort that $\mathbb{Z}[i]/2\mathbb{Z}[i]$ has order 4, and that the prime $\langle 1+i \rangle$ lying above 2 properly contains 2, so the size of $\mathbb{Z}[i]/\langle 1+i \rangle$ is a proper divisor of 4. Since $\langle 1+i \rangle \neq \mathbb{Z}[i]$, $\mathbb{Z}[i]/\langle 1+i \rangle$ has size 2. This is the same as $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$, so the inertia degree $f(\langle 1+i \rangle \mid 2) = 1$.

On the other hand, $3\mathbb{Z}[i]$ is prime and $\mathbb{Z}[i]/3\mathbb{Z}[i]$ has 9 elements, so $f(3\mathbb{Z}[i] \mid 3) = 2$.

A third type of example is $13\mathbb{Z}[i] = \langle 2+3i \rangle \langle 2-3i \rangle$; one can show that $\mathbb{Z}[i]/\langle 2+3i \rangle$ has 13 elements, so $f(\langle 2+3i \rangle \mid 13) = 1$.

These examples demonstrate a relationship between ramification degrees, inertia degrees, and the number of primes lying above a single rational prime, codified in the following fundamental result:

Proposition D.1.6. [46, Chapter 3, Theorem 21] Let $L/\mathbb{Q}$ be a number field, p a rational prime, and $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ the primes of L lying above p . Let $n = [L : \mathbb{Q}]$. Then

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

This result can be proved by analysing the ideal structure of rings of integers, similar to the proof of Proposition D.1.5.

In the above notation, the cases where the e_i , f_i , or g take extremal values are of particular interest:

Definition D.1.7. Let $L/\mathbb{Q}$ be a number field of degree n , and let p be a rational prime. Consider the factorisation $p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, and let f_i be the inertia degree of $\mathfrak{p}_i$ over p . The $(2g+1)$ -tuple of positive integers $(g, e_1, \dots, e_g, f_1, \dots, f_g)$ is called the **splitting**

pattern or splitting shape of p in L . There are also several special cases that are useful to define:

- If p has splitting pattern $(1, e_1, 1)$ in L , then by Proposition D.1.6, $e_1 = n$. In particular, $p\mathcal{O}_L = \mathfrak{p}_1^n$. In this case, we say that p is **totally ramified in L** .
- If p has splitting pattern $(1, 1, f_1)$ in L , then $f_1 = n$. Thus $p\mathcal{O}_L = \mathfrak{p}_1$, where $\mathfrak{p}_1$ has the maximum possible inertia degree. In this case, we say that p is **inert in L** .
- If p has splitting pattern $(g, 1, \dots, 1, 1, \dots, 1)$ in L , i.e., if $e_i = f_i = 1$ for all i , then $g = n$. In particular, $p\mathcal{O}_L = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, where each $\mathfrak{p}_i$ has the minimum possible inertia degrees. In this case, we say that p **splits completely in L** .

Example D.1.10. *Adding some terminology to Example D.1.9, in $\mathbb{Q}(i)$ we see that $\langle 1+i \rangle$ is totally ramified, $3\mathbb{Z}[i]$ is inert, and $13\mathbb{Z}[i]$ splits completely.*

We have avoided Galois theory so far, but its application to the study of number fields is hugely important. For example, it allows us to define algebraic invariants associated with prime ideal factorisations which give more detailed information than the discriminant. In fact, much of this follows from the fact that the Galois group of a Galois number field has a transitive action on a set with arithmetic significance:

Proposition D.1.7. *[52, Chapter I, Proposition 9.1] Let $L/\mathbb{Q}$ be a Galois number field, $G = \text{Gal}(L/\mathbb{Q})$ its Galois group, p a rational prime, and $S := \{\mathfrak{p}_1, \dots, \mathfrak{p}_g\}$ the set of primes of L lying above p . Then G acts transitively on S via the action*

$$\sigma \cdot \mathfrak{p}_i := \sigma(\mathfrak{p}_i).$$

The first consequence is the beautiful uniformity in prime ideal factorisations in Galois number fields:

Proposition D.1.8. *[52, Remarks preceding Chapter I, Proposition 9.3] Let $L/\mathbb{Q}$ be a Galois number field, p a rational prime, and $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ the primes of L lying above p . Then $e_i = e_j$ and $f_i = f_j$ for all i and j . In particular, denoting these common ramification and inertia degrees by e and f respectively, we have $efg = [L : \mathbb{Q}]$.*

Example D.1.11. *The field $L := \mathbb{Q}(\sqrt[3]{-23})$ is not Galois over $\mathbb{Q}$. One way to see this is to notice that the minimal polynomial of $\sqrt[3]{-23}$ over $\mathbb{Q}$ is $x^3 + 23$, and its two other roots are non-real complex numbers, while L is real. However, the contrapositive of Proposition D.1.8 allows us to see this as well, for*

$$2\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$$

for some primes $\mathfrak{p}_i$ of L , where $f(\mathfrak{p}_1 | 2) = 2$ but $f(\mathfrak{p}_2 | 2) = 1$.

Now, as alluded to above, we can attach a Galois-theoretic invariant due to the action of the Galois group on prime ideals.

Definition D.1.8. Let $L/\mathbb{Q}$ be a Galois number field with Galois group G . Let p be a rational prime, and $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ the primes of L lying above p . For each i , the **decomposition group of $\mathfrak{p}_i$ over p** , denoted by $D_L(\mathfrak{p}_i | p)$ or simply $D(\mathfrak{p}_i | p)$, is the stabiliser of $\mathfrak{p}_i$ under the action defined in Proposition D.1.7. Explicitly,

$$D_L(\mathfrak{p}_i | p) := D(\mathfrak{p}_i | p) := \{\sigma \in G : \sigma(\mathfrak{p}_i) = \mathfrak{p}_i\}.$$

Example D.1.12. The case of $L := \mathbb{Q}(i)$ is particularly simple, as the Galois group $G := \text{Gal}(L/\mathbb{Q})$ has order 2, with the non-trivial automorphism being complex conjugation, $i \mapsto -i$. Its only subgroups are thus trivial and G itself.

The only prime of L lying above 2 is $\langle 1+i \rangle$, so every automorphism in $\text{Gal}(L/\mathbb{Q})$ fixes $\langle 1+i \rangle$. Thus $D(\langle 1+i \rangle | 2)$ is the entire group G .

On the other hand, $13\mathcal{O}_L = \langle 2+3i \rangle \langle 2-3i \rangle$, so the primes above 13 are swapped by complex conjugation. Thus $D(\langle 2+3i \rangle | 13)$ and $D(\langle 2-3i \rangle | 13)$ are trivial.

Finally, $3\mathcal{O}_L$ is prime, so $D(3\mathcal{O}_L | 3)$ is all of G . However, we will see in Section D.3 that there is a difference between this case and the first case.

The following shows that decomposition groups contain information about both ramification and inertia, which can be proved with the orbit-stabiliser theorem:

Proposition D.1.9. [52, Remarks preceding Chapter I, Proposition 9.3] Let $L/\mathbb{Q}$ be a Galois number field. Let $\mathfrak{p}$ be a prime of L lying above the rational prime p . Then the size of the decomposition group $D(\mathfrak{p} | p)$ is $e(\mathfrak{p} | p)f(\mathfrak{p} | p)$.

We will use decomposition groups in Section D.3 to define Frobenius elements, which are attempts to leverage the wonderful properties of finite fields for the study of number fields.

D.2 Discriminants of Number Fields

The discriminant of a number field is one of the most important numerical invariant attached to a number field, as it contains all information about the field's ramified primes.

Our goal is to explain Proposition D.1.4, but along the way we will make some general definitions and state results which will be useful later.

As before, proofs are omitted, but we basically follow the logic of Conrad's expository notes on the subject ([18]). An alternative proof technique is spread across two chapters of Marcus's text ([46, Chapter 3, Theorem 24 and Chapter 4, Theorem 34]).

Definition D.2.1. Let B/A be an extension of (commutative, unital) rings, meaning that there is an injective ring homomorphism $A \rightarrow B$. Suppose that B is a free A -module of finite rank n , so that there exists a generating set $\mathcal{B} := \{\alpha_1, \dots, \alpha_n\}$ such that

$$B \cong A\alpha_1 \oplus \dots \oplus A\alpha_n.$$

as A -modules. For any $\alpha \in B$, the map $\mu_\alpha : B \rightarrow B$ denotes the multiplication by α map, which is an A -module homomorphism. The **trace of α over A** , or simply the **trace of α** , is denoted by $\text{Tr}_{B/A}(\alpha)$ or $\text{Tr}(\alpha)$, and is defined as the trace of the map μ_α . Note by definition that $\text{Tr}_{B/A}(\alpha) \in A$.

The trace of a ring extension turns out to have many applications in number theory and commutative algebra in general, some of which we will see soon. Another quantity with such applications is the following, which will return in Sections D.5 and D.6.

Definition D.2.2. Let B/A be an extension of rings such that B is a free A -module of finite rank. As in Definition D.2.1, let $\mu_\alpha : B \rightarrow B$ denote the multiplication by α map for any $\alpha \in B$. The **norm of α over A** , or simply the **norm of α** , is denoted by $N_{B/A}(\alpha)$ or $N(\alpha)$, and is defined as the determinant of the map μ_α . Note by definition that $N_{B/A}(\alpha) \in A$.

Note that it is common to define the trace and norm for field extensions only, but these general definitions will be useful for us, and the proofs of their important properties require basically no changes.

Example D.2.1. In $L := \mathbb{Q}(i)$, one can take the $\mathbb{Q}$ -basis $\mathcal{B} := \{1, i\}$. Let $\alpha := 1 - 2i$; then $\alpha \cdot 1 = \alpha$, and $\alpha \cdot i = 2 + i$, so the matrix $[\mu_\alpha]_{\mathcal{B}}$ is

$$\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}.$$

Thus, one sees that $\text{Tr}(\alpha) = 2$ and $N(\alpha) = 5$.

Let $L' := \mathbb{Q}(\sqrt[3]{-23})$, which has $\mathbb{Q}$ -basis $\mathcal{B}' := \{1, \sqrt[3]{-23}, \sqrt[3]{-23}^2\}$. For $\alpha' := \frac{2}{5} - \sqrt[3]{-23}$, we have

$$[\mu_{\alpha'}]_{\mathcal{B}'} = \begin{pmatrix} \frac{2}{5} & 23 & 0 \\ 0 & \frac{2}{5} & 23 \\ -1 & 0 & \frac{2}{5} \end{pmatrix}.$$

Thus, $\text{Tr}(\alpha') = \frac{6}{5}$ and $N(\alpha') = \frac{-66117}{125}$.

Example D.2.2. Let $L/\mathbb{Q}$ be a Galois number field, so that if $L = \mathbb{Q}(\theta)$ for some algebraic number θ , then the minimal polynomial of θ over $\mathbb{Q}$ splits into distinct linear factors over L . Now let $\alpha \in L$ and write $\alpha_1 := \alpha, \alpha_2, \dots, \alpha_n$ for the elements of L which have the same minimal polynomial as α , which we call the **Galois conjugates of α in L** . Then one can show ([52, Chapter I, Proposition 2.6]) that $\text{Tr}(\alpha) = \sum_{i=1}^n \alpha_i$ and $N(\alpha) = \prod_{i=1}^n \alpha_i$.

For example, in $\mathbb{Q}(\sqrt{2})$, the other Galois conjugate of $\alpha := a + b\sqrt{2}$ is $\alpha_2 := a - b\sqrt{2}$, so $\text{Tr}(\alpha) = 2a$ and $N(\alpha) = a^2 - 2b^2$.

Proposition D.2.1. [52, Chapter I, remarks preceding Proposition 2.6] Let B/A be a ring extension such that B is a free A -module of finite rank, say n . Then Tr is an A -module homomorphism, and N is multiplicative. Explicitly, for $\alpha, \beta \in B$ and $s \in A$, $\text{Tr}(s\alpha + \beta) = s \text{Tr}(\alpha) + \text{Tr}(\beta)$ and $N(\alpha\beta) = N(\alpha)N(\beta)$. In particular, if $\alpha \in A$, then $\text{Tr}(\alpha) = n\alpha$ and $N(\alpha) = \alpha^n$.

The following says that, in the case of a number field, the trace and norm can detect integrality.

Proposition D.2.2. [46, Chapter 2, Corollary 2] Let $L/\mathbb{Q}$ be a number field. If $\alpha \in \mathcal{O}_L$, then $\text{Tr}(\alpha) \in \mathbb{Z}$ and $N(\alpha) \in \mathbb{Z}$.

Now we are ready to define the discriminant of a ring extension with respect to a chosen generating set.

Definition D.2.3. Let B/A be a ring extension such that B is a free A -module of finite rank. Let $\mathcal{B} := \{\alpha_1, \dots, \alpha_n\}$ be a generating set of B as an A -module. The **discriminant of $\mathcal{B}$ over A** , or simply the **discriminant of $\mathcal{B}$** , is denoted by $\text{disc}_A(\mathcal{B})$ and is defined as the determinant

$$\text{disc}_A(\mathcal{B}) := \det \begin{pmatrix} \text{Tr}_{B/A}(\alpha_1^2) & \text{Tr}_{B/A}(\alpha_1\alpha_2) & \cdots & \text{Tr}_{B/A}(\alpha_1\alpha_n) \\ \text{Tr}_{B/A}(\alpha_1\alpha_2) & \text{Tr}_{B/A}(\alpha_2^2) & \cdots & \text{Tr}_{B/A}(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \text{Tr}_{B/A}(\alpha_1\alpha_n) & \text{Tr}_{B/A}(\alpha_2\alpha_n) & \cdots & \text{Tr}_{B/A}(\alpha_n^2) \end{pmatrix} \quad (\text{D.1})$$

This definition may seem arbitrary, but is natural in light of the fact that the map

$$B \times B \rightarrow A,$$

$$(\alpha, \beta) \mapsto \text{Tr}(\alpha\beta)$$

defines a non-degenerate bilinear form similar to the standard dot product on $\mathbb{R}^n$ or $\mathbb{C}^n$, meaning that the matrix (D.1) is the Gram matrix of this “tracial” bilinear form. This also allows one to interpret the discriminant as a “volume”, as with the determinant of a general linear map.

Example D.2.3. From Example D.1.3, we saw that a $\mathbb{Z}$ -generating set of $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$ is $\mathcal{B}_1 := \{1, i\}$. Skipping the trace computations, the relevant matrices of $\mathcal{B}_1$ and $\mathcal{B}_2$ are, respectively,

$$\begin{pmatrix} \text{Tr}(1) & \text{Tr}(i) \\ \text{Tr}(i) & \text{Tr}(-1) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$$

and

$$\begin{pmatrix} \text{Tr}(2i) & \text{Tr}(-1+i) \\ \text{Tr}(-1+i) & \text{Tr}(-1) \end{pmatrix} = \begin{pmatrix} 0 & -2 \\ -2 & -2 \end{pmatrix}.$$

Thus, we see that $\text{disc}_{\mathbb{Z}}(\mathcal{B}_1) = \text{disc}_{\mathbb{Z}}(\mathcal{B}_2) = -4$. This is not a coincidence!

Example D.2.4. Let $L/\mathbb{Q}$ be a number field, so that $\mathcal{O}_L$ is a free $\mathbb{Z}$ -module of rank $n := [L : \mathbb{Q}]$. If $\mathcal{B} := \{\alpha_1, \dots, \alpha_n\}$ is a $\mathbb{Z}$ -generating set of $\mathcal{O}_L$, then for any $m \in \mathbb{Z}$, it is a standard commutative algebra fact that $\mathcal{O}_L/m\mathcal{O}_L$ is a free $\mathbb{Z}/m\mathbb{Z}$ -module of rank n with generating set $\overline{\mathcal{B}} := \{\alpha_1 + m\mathcal{O}_L, \dots, \alpha_n + m\mathcal{O}_L\} =: \{\overline{\alpha}_1, \dots, \overline{\alpha}_n\}$.

As a specific example, let $L = \mathbb{Q}(\sqrt[3]{-23})$, whose ring of integers is $\mathbb{Z}[\sqrt[3]{-23}]$. A $\mathbb{Z}$ -generating set is $\mathcal{B} := \{1, \sqrt[3]{-23}, \sqrt[3]{-23}^2\}$, so an $\mathbb{F}_5$ -generating set is $\mathcal{B}_5 := \{1 + 5\mathcal{O}_L, \sqrt[3]{-23} + 5\mathcal{O}_L, \sqrt[3]{-23}^2 + 5\mathcal{O}_L\}$. Noting that $-23 \equiv 2 \pmod{5}$, routine computation shows that $\text{disc}_{\mathbb{F}_5}(\mathcal{B}_5) = 2$.

Repeating the above for $\mathbb{F}_3$ shows that $\text{disc}_{\mathbb{F}_3}(\mathcal{B}_3) = 0$.

The following result pulls double weight: First, it says that the equation $\text{disc}_A(\mathcal{B}) = 0$ is independent of the choice of generating set $\mathcal{B}$, and fortunately this is the most important property of a discriminant that we will need to check in general. Second, it says that in the special case of the ring of integers of a number field, the discriminant over $\mathbb{Z}$ is independent of the choice of generating set.

Proposition D.2.3. [18, Remarks preceding Lemma 3.3] Let B/A be a ring extension such that B is a free, finite-rank A -module, and let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two A -generating sets of B . Then $\text{disc}_A(\mathcal{B}_1)$ and $\text{disc}_A(\mathcal{B}_2)$ differ by the square of a unit in $A^\times$.

Now we can define one of the most fundamental invariants associated with a number field.

Definition D.2.4. Let $L/\mathbb{Q}$ be a number field. The **discriminant of L** , denoted by $\text{disc}(L)$, is the discriminant of any (hence, every) $\mathbb{Z}$ -generating set of $\mathcal{O}_L$.

Example D.2.5. Example D.2.3 shows that $\text{disc}(\mathbb{Q}(i)) = -4 = -2^2$. In general, one can show ([46, Chapter 2, preceding Theorem 12]) that

$$\text{disc}(\mathbb{Q}(\sqrt{d})) = \begin{cases} d, & \text{if } d \equiv 1 \pmod{4} \\ 4d, & \text{if } d \not\equiv 1 \pmod{4} \end{cases}$$

For readers familiar with polynomial discriminants, note that one can always take $x^2 - d$ as a defining polynomial of $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, but the discriminant of this polynomial is not equal to the corresponding field discriminant when $d \equiv 1 \pmod{4}$.

In any case, this covers all possible number fields of degree 2. Degree-3 fields are more varied, but for example, one can show that $\text{disc}(\mathbb{Q}(\sqrt[3]{-23})) = -14,283 = -3^3 \cdot 23^2$. The final result of this section explains why it is useful to give discriminants in terms of their prime factorisations. For now, one may notice that 3 divides $\text{disc}(\mathbb{Q}(\sqrt[3]{-23}))$, and that from Example D.2.4, the discriminant of $\mathcal{O}_L/3\mathcal{O}_L$ as a ring extension of $\mathbb{F}_3$ vanished.

The next result generalises the observations concerning $\mathbb{Q}(\sqrt[3]{-23})$ from Examples D.2.4 and D.2.5:

Lemma D.2.1. [18, Lemma 3.3] Let $L/\mathbb{Q}$ be a number field and $\mathfrak{p}$ a prime of L lying above the rational prime p . Then there exists a $\mathbb{Z}$ -basis $\mathcal{B}_{\mathbb{Z}}$ of $\mathcal{O}_L$, and an $\mathbb{F}_p$ -basis $\mathcal{B}_p$ of $\mathcal{O}_L/\langle p \rangle$, such that $\text{disc}_{\mathbb{Z}}(\mathcal{B}_{\mathbb{Z}})$ is congruent to $\text{disc}_{\mathbb{F}_p}(\mathcal{B}_p)$ modulo p .

In fact, this is the central puzzle piece which explains the utility of discriminants for studying number fields, and also shows that almost all rational primes are unramified in a given number field:

Theorem D.2.1. [18, Theorem 1.3] Let $L/\mathbb{Q}$ be a number field. Then a rational prime p ramifies in L if and only if $p \mid \text{disc}(L)$. In particular, since $\text{disc}(L)$ is non-zero, there are only finitely many rational primes which ramify in L .

D.3 Frobenius Elements of Number Fields

Frobenius elements are fundamental constructions in algebraic number theory. At a very high level, they connect external information, i.e., field extensions, with internal informa-

tion, i.e., *ideal class groups*. This is particularly fruitful in the case of a number field whose Galois group is Abelian, but also has beautiful applications in the general case, such as the proof of Theorem 1.2.2.

The goal of this section is to describe Frobenius elements in enough detail to allow the reader to follow the final proof of Section 2.2. As a secondary goal, we state the famous Chebotarev Density Theorem concerning the statistical distribution of Frobenius elements.

The main reference for results on Frobenius elements is Marcus ([46, Chapter 4]). The pre-requisites for understanding a proof of the Chebotarev Density Theorem are much more advanced than the previous background sections, so for brevity, we do not treat them in this thesis. A standard reference for this material is Neukirch ([52, Chapter VII, Section 13]).

As mentioned in the previous section, Frobenius elements are attempts to import structure from extensions of finite fields to number fields.

Definition D.3.1. Let ℓ/k be a finite-degree field extension of finite fields. Suppose that $|k| = q$, which is necessarily a prime power. Then the map

$$\ell \rightarrow \ell, \quad \alpha \mapsto \alpha^q$$

is an element of $\text{Gal}(\ell/k)$, and in fact is a generator of $\text{Gal}(\ell/k)$. This is called the **Frobenius element of ℓ/k** , denoted by $\text{Frob}(\ell/k)$.

Example D.3.1. Let $\text{GF}(8)$ denote a finite field of order $8 = 2^3$, which can be constructed as a quotient of $\mathbb{F}_2[x]$ and is unique up to (non-canonical) isomorphism. Then $\text{GF}(8)/\mathbb{F}_2$ has degree 3, and the map

$$\text{GF}(8) \rightarrow \text{GF}(8), \quad \alpha \mapsto \alpha^2$$

is the Frobenius element of $\text{GF}(8)/\mathbb{F}_2$.

Note, the definition of the Frobenius element of an extension of finite fields relies on three distinguishing features of such extensions: First, the map $\alpha \mapsto \alpha^q$ is a ring homomorphism, where q is the size of the ground field. Second, the ground field is fixed by this homomorphism (a consequence of Fermat's Little Theorem). And third, such an extension is always Galois with cyclic Galois group.

The key ingredients to pull this structure back to a number field are the decomposition groups from Section D.1:

Proposition D.3.1. [46, Chapter 4, preceding Theorem 28] Let $L/\mathbb{Q}$ be a Galois number field and $\mathfrak{p}$ a prime of L lying above the rational prime p . Then the map

$$D(\mathfrak{p} \mid p) \rightarrow \text{Gal}((\mathcal{O}_L/\mathfrak{p})/\mathbb{F}_p),$$

$$\sigma \mapsto \bar{\sigma}$$

given by, for $\alpha \in L$,

$$\bar{\sigma}(\alpha + \mathfrak{p}) := \sigma(\alpha) \pmod{p}$$

is a well-defined surjective group homomorphism.

Note that it is exactly the definition of $D(\mathfrak{p} \mid p)$ which guarantees well-definition of the above map. Surjectivity now allows us to select elements from $D(\mathfrak{p} \mid p) \leq \text{Gal}(L/\mathbb{Q})$ which behave like Frobenius elements of finite fields.

Definition D.3.2. Let $L/\mathbb{Q}$ be a Galois number field and $\mathfrak{p}$ a prime of L lying above the rational prime p . A **Frobenius element of $\mathfrak{p}$** is any automorphism $\sigma \in D(\mathfrak{p} \mid p)$ in the pre-image of $\text{Frob}((\mathcal{O}_L/\mathfrak{p})/\mathbb{F}_p)$ under the map from Proposition D.3.1, i.e., any σ such that $\bar{\sigma}$ acts as the p^{th} -power map on $\mathbb{F}_p$.

Of course, since the map from Proposition D.3.1 may not be injective, there may be ambiguity in the choice of an element of the fibre of $\text{Frob}((\mathcal{O}_L/\mathfrak{p})/\mathbb{F}_p)$. This is captured by the kernel of this map:

Definition D.3.3. Let $L/\mathbb{Q}$ be a Galois number field with Galois group G , and let $\mathfrak{p}$ be a prime of L lying over the rational prime p . The kernel of the map defined in Proposition D.3.1 is called the **inertia group of $\mathfrak{p}$ over p** , denoted by $I_L(\mathfrak{p} \mid p)$ or simply $I(\mathfrak{p} \mid p)$. Thus, $I(\mathfrak{p} \mid p)$ is a subgroup of G and a normal subgroup of $D(\mathfrak{p} \mid p)$.

So, a Frobenius element of a prime $\mathfrak{p}$ may only be defined up to multiplication by an element of $I(\mathfrak{p} \mid p)$. Fortunately, for a given Galois number field $L/\mathbb{Q}$, almost all rational primes - specifically, the unramified ones - will have a unique Frobenius element in $\text{Gal}(L/\mathbb{Q})$.

Proposition D.3.2. Let $L/\mathbb{Q}$ be a Galois number field and $\mathfrak{p}$ a prime of L lying above the rational prime p . Then the size of the inertia group $I(\mathfrak{p} \mid p)$ is equal to the ramification degree $e(\mathfrak{p} \mid p)$. In particular, if p is unramified in L then there is a unique Frobenius element of $\mathfrak{p}$, denoted by $\text{Frob}_L(\mathfrak{p} \mid p)$ or $\text{Frob}(\mathfrak{p} \mid p)$.

Proof. A direct consequence of Proposition D.1.9. □

Example D.3.2. In Example D.1.12, we saw that in $L := \mathbb{Q}(i)$, since 2 is totally ramified and 3 is inert, the decomposition groups $D(\langle 1+i \rangle \mid 2)$ and $D(3\mathcal{O}_L \mid 3)$ are both equal to the entire Galois group G . However, by Proposition D.3.2, these two primes have different inertia groups: $I(\langle 1+i \rangle \mid 2)$ is also all of G , while $I(3\mathcal{O}_L \mid 3)$ is trivial.

Example D.3.3. Let $n \geq 1$ and $\zeta_n := e^{2\pi i/n}$, a primitive n^{th} root of unity. Then $L := \mathbb{Q}(\zeta_n)$ is called the n^{th} **cyclotomic field**, which by standard field theory is Galois over $\mathbb{Q}$ of degree $\varphi(n)$ (the Euler totient function of n), with Galois group $G := (\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative group of congruence classes modulo n which are coprime to n . In fact, the elements of G are all of the form $\zeta_n \mapsto \zeta_n^k$ for some $1 \leq k < n$. In particular, $L/\mathbb{Q}$ is Abelian, i.e., has Abelian Galois group.

One can show ([46, Chapter 4, following Theorem 32]) that $\mathcal{O}_L = \mathbb{Z}[\zeta_n]$ and that $L/\mathbb{Q}$ is unramified at every prime not dividing n , and also at 2 if $n \equiv 2 \pmod{4}$.

Let us specialise to the case $n = 5$, so that $L/\mathbb{Q}$ is Galois of degree 4 with Galois group C_4 . Then 2, 3, and 13 are inert, 5 is totally ramified, and 11 is completely split. Thus by size arguments, $D(2\mathcal{O}_L \mid 2) = D(3\mathcal{O}_L \mid 3) = D(13\mathcal{O}_L \mid 13) = D(\mathfrak{p}_1 \mid 5) = G$, while $D(\mathfrak{p}_i \mid 11)$ is trivial, where $\mathfrak{p}_1$ is the prime above 5 and $\mathfrak{p}_2, \dots, \mathfrak{p}_5$ are the primes above 11.

With a modest amount of effort, one finds that each unramified rational prime mentioned above has a unique Frobenius element: $\text{Frob}(2\mathcal{O}_L \mid 2)$ is the automorphism $\zeta_5 \mapsto \zeta_5$, $\text{Frob}(3\mathcal{O}_L \mid 3)$ is $\zeta_5 \mapsto \zeta_5^3$, and $\text{Frob}(13\mathcal{O}_L \mid 13)$ is $\zeta_5 \mapsto \zeta_5^{-1}$, while $\text{Frob}(\mathfrak{p}_i \mid 11)$ is the trivial map between two trivial groups. This turns out to be a consequence of $L/\mathbb{Q}$ being Abelian, as we will soon see.

Also notice that for each element σ of G , there is an unramified rational prime such that σ is its Frobenius element. This is a special case of the Chebotarev Density Theorem, to be stated later.

In general, above a given rational prime p , there may be several primes of $L/\mathbb{Q}$ lying above p , hence several Frobenius elements associated with p . However, the transitive action of $\text{Gal}(L/\mathbb{Q})$ on this set of primes (see Proposition D.1.7) confines them together in the following sense:

Proposition D.3.3. Let $L/\mathbb{Q}$ be a Galois number field with Galois group G , and let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be primes of L lying over the same rational prime p . If p is unramified in L , then $\text{Frob}(\mathfrak{p}_1 \mid p)$ and $\text{Frob}(\mathfrak{p}_2 \mid p)$ are conjugates of each other in G . In particular, if $\sigma \in G$ satisfies $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$, then $\sigma^{-1} \text{Frob}(\mathfrak{p}_2 \mid p) \sigma = \text{Frob}(\mathfrak{p}_1 \mid p)$.

Definition D.3.4. Let $L/\mathbb{Q}$ be a Galois number field, $G := \text{Gal}(L/\mathbb{Q})$, p a rational prime which is unramified in L , and $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ the primes of L lying above p . The **Frobenius class of p** , denoted by $\text{Frob}_L(p)$ or $\text{Frob}(p)$, is the conjugacy class of G with elements $\{\text{Frob}_L(\mathfrak{p}_1 \mid p), \dots, \text{Frob}_L(\mathfrak{p}_g \mid p)\}$.

This explains the remark at the end of Example D.3.3 that Abelian Galois groups are easy to work with, as then each Frobenius class is a singleton.

There is more that can be said in the unramified case, which begins to show the utility of computing Frobenius elements:

Corollary D.3.1. *[46, Chapter 4, following Theorem 32] Let $L/\mathbb{Q}$ be a Galois number field, and p an unramified rational prime in L . Then each element of $\text{Frob}(p)$ has order f , the inertia degree of any (hence, every) prime of L above p .*

Proof. In this case, $D(\mathfrak{p} \mid p)$ (for any $\mathfrak{p}$ above p) is isomorphic to $\text{Gal}((\mathcal{O}_L/\mathfrak{p})/\mathbb{F}_p)$, which is cyclic of order f , and $\text{Frob}(\mathfrak{p} \mid p)$ must be mapped to a generator. $\square$

Another result that will be useful is the connection between Frobenius elements as permutations (when the ambient Galois group is embedded in some symmetric group) and factorisations of polynomials modulo primes. This gives some intuition for the appearance of Frobenius elements in the proof of Theorem 1.2.2.

The proof is a surprisingly straightforward application of finite field theory.

Proposition D.3.4. *[19, Theorem 1] Let $f(x) \in \mathbb{Z}[x]$ be monic and irreducible with $\deg(f) = n$. Let $L/\mathbb{Q}$ be a splitting field of f , so that $L/\mathbb{Q}$ is a Galois extension. Embed $G := \text{Gal}(L/\mathbb{Q})$ into S_n via its actions on the roots of $f(x)$, which defines G as a subgroup of S_n up to conjugation in S_n .*

For a rational prime p which is unramified in L , let

$$f_p(x) = \pi_{p,1}(x) \cdots \pi_{p,k_p}(x) \in \mathbb{F}_p[x]$$

be the factorisation of $f(x)$ into distinct, monic irreducibles over $\mathbb{F}_p$. Then every element of the Frobenius class $\text{Frob}_L(p)$ of p has cycle type

$$(\deg(\pi_{p,1}), \dots, \deg(\pi_{p,k_p})).$$

In other words, for any element of $\text{Frob}_L(p)$, the number of disjoint cycles in its cycle decomposition is equal to the number k_p of irreducible factors of $f(x)$ when reduced modulo p , and moreover, the cycles and irreducible factors can be rearranged so that the i^{th} cycle has length equal to the degree of the i^{th} irreducible factor.

Example D.3.4. Let $\varphi(x) := x^2 + x + 1$; note that its splitting field is the 3rd cyclotomic field (see Example D.3.3), which can be generated as $L := \mathbb{Q}(\sqrt{-3})$. In particular, $L/\mathbb{Q}$ is of degree 2, hence its Galois group is C_2 , which is cyclic (and therefore Abelian).

In L , note that 2 is inert, while 7 splits completely. A similar analysis to Example D.3.3 shows that the generator of C_2 is the Frobenius above 2, while the identity automorphism

is the Frobenius above 7. Correspondingly, we have the factorisations

$$\varphi_2(x) := x^2 + x + 1 \in \mathbb{F}_2[x],$$

$$\varphi_7(x) := (x + 3)(x + 5) \in \mathbb{F}_7[x].$$

Example D.3.5. Consider the polynomial $f(x) := x^3 - 19 \in \mathbb{Z}[x]$, which is irreducible, and let $L/\mathbb{Q}$ be a splitting field, which can be constructed as $L = \mathbb{Q}(\sqrt[3]{19}, \sqrt{-3})$ and has degree 6 over $\mathbb{Q}$. Now the factorisations of $2\mathcal{O}_L$ and $7\mathcal{O}_L$ are

$$2\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$$

and

$$7\mathcal{O}_L = \mathfrak{p}_4\mathfrak{p}_5,$$

where the primes above 2 all have inertia degree 2, and those above 7 all have degree 3 (as forced by Proposition D.1.8). The factorisations of $f(x)$ modulo 2 and 7 are

$$f_2(x) = (x + 1)(x^2 + x + 1) \in \mathbb{F}_2[x],$$

$$f_7(x) = x^3 + 2 \in \mathbb{F}_7[x].$$

Thus, the actions of the Frobenius elements of 2 and 7 on the roots of f are, respectively, a 2-cycle (with the linear factor modulo 2 corresponding to a root of f which is fixed) and a 3-cycle.

In fact, since 2 and 7 are unramified, all of their decomposition groups in G are cyclic of sizes 2 and 3 (respectively), and they are isomorphic to the corresponding Galois groups of finite fields. This means that any 2-cycle in S_3 will serve as a Frobenius element above 2, and similarly for 3-cycles above 7.

Notice that the splitting field in this example contains that of the previous example as an intermediate extension. Further, the behaviours of $\varphi(x)$ and $f(x)$ have “complementary” behaviours in the sense that $\varphi(x)$ has a root modulo 7 but remains irreducible modulo 2, while $f(x)$ has a root modulo 2 and is irreducible modulo 7. This relationship turns out to hold for all unramified primes in $\mathbb{Q}(\sqrt[3]{19}, \sqrt{-3})$, and in fact is key to the intersectivity of the polynomial $(x^3 - 19)(x^2 + x + 1)$.

It is hard to finish a discussion on Frobenius elements without stating the celebrated Chebotarev Density Theorem, which is a statistical result on splitting patterns of unramified primes and their possible Frobenius elements. There are at least two proof methods, with and without the machinery of Class Field Theory; see, respectively, Neukirch’s text

([52, Chapter VII, Section 13]) and the survey article by Lenstra and Stevenhagen ([43, Appendix]). We will finish by stating three important consequences.

First, it is helpful to make the following definition:

Definition D.3.5. Let S be a subset of $\mathbb{Z}_{>0}$. The **natural density** or **asymptotic density** of S is defined as the limit

$$\lim_{n \rightarrow \infty} \frac{|\{a \in S : a \leq n\}|}{n},$$

when this limit exists. In other words, the natural density of S is the asymptotic ratio of positive integers which are in S .

Theorem D.3.1. [52, Chapter VII, Theorem 13.4] *Let $L/\mathbb{Q}$ be a Galois number field with Galois group $G := \text{Gal}(L/\mathbb{Q})$. Let S be a subset of G which is closed under conjugation. Then the set of rational primes which are unramified in L and whose Frobenius class is contained in S has natural density*

$$\frac{|S|}{|G|}.$$

Intuitively, Chebotarev Density says that the proportion of primes which are unramified in L and with specified Frobenius class is precisely quantified by the proportion of automorphisms in $\text{Gal}(L/\mathbb{Q})$ lying in that conjugacy class.

Example D.3.6. *Let $L/\mathbb{Q}$ be a Galois number field with $G := \text{Gal}(L/\mathbb{Q}) \cong S_3$. Conjugacy in S_3 is the same as cycle type when permutations are decomposed into disjoint cycles; in particular, there are exactly three conjugacy classes in S_3 :*

$$\{\text{id}\}, \quad \{(1, 2, 3), (1, 3, 2)\}, \quad \text{and} \quad \{(1, 2), (1, 3), (2, 3)\}.$$

Chebotarev Density says that these classes partition the Frobenius elements of unramified primes in L . More explicitly, $\frac{1}{|S_3|} = \frac{1}{6}$ of such primes have trivial Frobenius class, $\frac{1}{3}$ of them have the Frobenius class of a 3-cycle, and $\frac{1}{2}$ of them have the Frobenius class of a 2-cycle.

By Corollary D.3.1, we can translate this to statistical information about splitting patterns of unramified primes in L : $\frac{1}{6}$ of such primes are split completely, $\frac{1}{3}$ of them lie below two primes of inertia degree 3, and $\frac{1}{2}$ of them lie below three primes of inertia degree 2.

The following are straightforward consequences of Chebotarev Density which connect the arithmetic information of Frobenius elements with the algebraic structure of Galois groups:

Corollary D.3.2. *Let $L/\mathbb{Q}$ be a Galois number field with Galois group G , and let C be a conjugacy class of elements in G . Then there are infinitely many rational primes which are unramified in L whose Frobenius class is equal to C . In particular, every conjugacy class of G can be viewed as the Frobenius class of infinitely many unramified rational primes in L .*

Corollary D.3.3. *Let $L/\mathbb{Q}$ be a Galois number field with Galois group G , and let $n = [L : \mathbb{Q}] = |G|$. Suppose that G has an element of order f . Then there are infinitely many rational primes which are unramified in L and which lie below $\frac{n}{f}$ primes of L , each having inertia degree f . In particular, if G is not cyclic, then no rational primes are unramified and inert in L .*

The following is also surprisingly straightforward to prove and demonstrates the vast power of Chebotarev Density:

Corollary D.3.4. *[52, Chapter VII, Theorem 13.10] Let $L/\mathbb{Q}$ be a Galois number field. Then L is uniquely determined by the set of rational primes which split completely in it.*

This Corollary means that splitting patterns of prime ideals contains exactly as much mathematical information as the entire set of Galois number fields, so it is not surprising that the former is so incredibly rich.

D.4 The p -Adic Integers and p -Adic Numbers

The goal of this section is to establish the equivalence between polynomial roots in the p -adic integers $\mathbb{Z}_p$, where p is a prime, and roots modulo all powers of p . A secondary goal is to establish its field of fractions $\mathbb{Q}_p$ and the various algebraic properties of them.

There are many equivalent ways to define $\mathbb{Z}_p$; we define it as the set of sequences of congruence classes modulo progressively higher powers of p , subject to a compatibility condition between components. This compatibility condition will ensure that every p -adic integer is a limit of an integer, i.e., that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ - more on this later. This will also ensure that “most” p -adic integers are invertible, making the formation of $\mathbb{Q}_p$ a simple procedure.

No specific background is assumed for this section, except familiarity with standard topological results. The main reference is the set of lecture notes for MIT’s 18.782 course by Chidambaram, specifically lectures 4–10 ([15]). Some other references are Chapter II of Neukirch’s text ([52]) and Serre’s text ([60]).

To see the forest for the trees, the reader should keep in mind the “purpose” of constructing $\mathbb{Z}_p$: It is a topological ring with an interesting (i.e., non-discrete) topology in which every element can be approximated by integers; moreover, the topology contains arithmetic information, namely divisibility information for all powers of p , and no other arithmetic information.

Definition D.4.1. Let $p \in \mathbb{Z}$ be a prime number. A **p -adic integer** is an element α of the direct product $\prod_{i \geq 1} \mathbb{Z}/p^i\mathbb{Z}$ such that $\varphi_i(\alpha_{i+1}) = \alpha_i$, where $\varphi_i : \mathbb{Z}/p^{i+1}\mathbb{Z} \rightarrow \mathbb{Z}/p^i\mathbb{Z}$ is the canonical projection map. The set of all p -adic integers is denoted by $\mathbb{Z}_p$.

Example D.4.1. For $p = 7$, some examples of 7-adic integers are

$$(0, 7, 7, 7, \dots)$$

and

$$(6, 13, 111, 111, 111, \dots).$$

We will see that these correspond, respectively, to the integers 7 and 111, assuming that no surprises are hidden in the ellipses. A 7-adic integer which does not correspond to an integer may begin as follows:

$$(6, 13, 111, 565, \dots).$$

On the other hand, the following is not a 7-adic integer due to the incompatibility between the first and second components:

$$(6, 14, 112, 566, \dots).$$

Intuitively, for $m \in \mathbb{Z}$, specifying the congruence class of m modulo the prime p gives accuracy $\frac{1}{p}$. In other words, one in p integers will share the same congruence class. Further specifying the class of m modulo p^2 gives more accuracy, namely, only one in p^2 integers share that congruence class. Hence for integers, looking at further components of its corresponding sequence in $\mathbb{Z}_p$ gives more information on its true value. This will turn out to be true for proper p -adic integers as well.

One advantage of this definition of $\mathbb{Z}_p$ is the simplicity of the algebraic operations, with closure following by homomorphicity of the projections φ_i :

Proposition D.4.1. Let $p \in \mathbb{Z}$ be prime. The set of p -adic integers $\mathbb{Z}_p$, with operations defined componentwise, is a subring of $\prod_{i \geq 1} \mathbb{Z}/p^i\mathbb{Z}$.

Fortunately, this is compatible with the existing structure in $\mathbb{Z}$:

Proposition D.4.2. [15, Lecture 4, preceding Example 4.4] Let $p \in \mathbb{Z}$ be prime. The map $\mathbb{Z} \rightarrow \mathbb{Z}_p$ sending an integer to its reduction modulo p^n for each $n \geq 1$ is an injective ring homomorphism.

Example D.4.2. Proposition D.4.2 makes sense of the claim from Example D.4.1 that the 7-adic integer

$$(6, 13, 111, 111, 111, \dots)$$

corresponds to the integer 111.

Example D.4.3. For $n \geq 1$, let us see what the integer p^n looks like in $\mathbb{Z}_p$. Indeed, using Proposition D.4.2, since p^n is divisible by all smaller powers of p , p^n embeds in $\mathbb{Z}_p$ as

$$(0, 0, \dots, 0, 0, p^n, p^n, p^n, \dots),$$

where the final 0 is in the $(n+1)^{\text{st}}$ component. In a sense (to be made precise later), p^n is a p -adic integer which approximates 0 with exactly n components of accuracy, so it is reasonable to call p^n a “ p -adically small” integer.

Another advantage of our setup is that the following fact is easily proved:

Proposition D.4.3. [15, Lecture 4, Theorem 4.8] For any $n \geq 1$, the projection map $\pi_n : \mathbb{Z}_p \rightarrow \mathbb{Z}/p^n\mathbb{Z}$ onto the n^{th} component is a surjective ring homomorphism, and its kernel is the principal ideal $p^n\mathbb{Z}_p$.

This gives us, for every $n \geq 1$, the short exact sequence

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{\cdot p^n} \mathbb{Z}_p \xrightarrow{\pi_n} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0,$$

and the following is an easy consequence:

Corollary D.4.1. For any $n \geq 1$, $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

It is helpful to now define the the p -adic numbers $\mathbb{Q}_p$; a natural construction is enabled by the following pleasant algebraic structure.

Proposition D.4.4. [15, Lecture 4, Theorem 4.15(1) and Corollary 4.17] Let $p \in \mathbb{Z}$ be prime. Then every element of $\mathbb{Z}_p$ which is not divisible by p is a unit in $\mathbb{Z}_p$. In other words, the set of non-units in $\mathbb{Z}_p$ is exactly the principal ideal $p\mathbb{Z}_p$. As a consequence, $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$, so that $\mathbb{Z}_p$ is a local ring.

This justifies the term “Local-to-Global Principle” in number theory. This also further cements the idea that $\mathbb{Z}_p$ focuses on a single prime at a time, as the other prime ideals of $\mathbb{Z}$ - generated by primes other than p - are now the unit ideal in $\mathbb{Z}_p$.

Definition D.4.2. The **field of p -adic numbers**, $\mathbb{Q}_p$, is defined as the localisation of $\mathbb{Z}_p$ at p . In other words, we adjoin a multiplicative inverse of p to $\mathbb{Z}_p$. In symbols:

$$\mathbb{Q}_p := \mathbb{Z}_p [p^{-1}].$$

In particular, elements of $\mathbb{Q}_p$ are formal fractions of the form $\frac{a}{p^k}$ where $a \in \mathbb{Z}_p$ and $k \geq 0$. Addition and multiplication are defined as

$$\frac{a}{p^k} + \frac{a'}{p^{k'}} := \frac{ap^{k'} + a'p^k}{p^{k+k'}},$$

$$\frac{a}{p^k} \cdot \frac{a'}{p^{k'}} := \frac{aa'}{p^{k+k'}}.$$

Even more explicitly, an element of $\mathbb{Q}_p$ can be viewed as a sequence in $\mathbb{Z}_p$, possibly multiplied by some negative power of p :

$$p^{-k}(a_1, a_2, a_3, \dots), \quad k \geq 0.$$

The implicit proposition that $\mathbb{Q}_p$ is a field follows from Proposition D.4.4.

We now start to rigorously define the notion of size implied in Example D.4.3. It will be helpful later to give these ideas in more generality.

Definition D.4.3. Let A be an integral domain. A **valuation on A** is a map

$$\nu : A \rightarrow \mathbb{R} \cup \{\infty\},$$

where ∞ is a formal symbol such that $x + \infty = \infty$ and $x < \infty$ for all $x \in \mathbb{R}$, with the condition that $\nu(\alpha) = \infty \iff \alpha = 0$. The image $\nu(A \setminus \{0\})$, which is an additive subgroup of $\mathbb{R}$, is called the **value group of A** . A **discrete valuation on A** is a valuation such that, for all $\alpha, \beta \in A$,

1. The value group $\nu(A \setminus \{0\})$ is a discrete subgroup of $\mathbb{R}$, i.e., of the form $r\mathbb{Z}$ for some $r \in \mathbb{R}$.
2. $\nu(\alpha\beta) = \nu(\alpha) + \nu(\beta)$.

$$3. \nu(\alpha + \beta) \geq \min\{\nu(\alpha), \nu(\beta)\}.$$

The third property above is called the **ultrametric inequality** or **non-Archimedean property**.

The non-Archimedean property is responsible for most of the interesting properties of $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

The following generalises the relationship between $\mathbb{Z}_p$ and $\mathbb{Q}_p$, and in Section D.5, we will also see analogies with rings of integers of number fields (see Definition D.1.2):

Proposition D.4.5. *[60, Chapter 1, Proposition 1 and preceding remarks] Let A be an integral domain with discrete valuation ν . Let K be the field of fractions of A . Then ν can be extended uniquely to a discrete valuation on K , which by abuse of notation we also call ν . Explicitly, writing an element of K as $\frac{\alpha}{\beta}$ for $\alpha \in A$ and $\beta \in A \setminus \{0\}$, we define*

$$\nu\left(\frac{\alpha}{\beta}\right) := \nu(\alpha) - \nu(\beta).$$

In this case, A is exactly the subring

$$A = \{\alpha \in K : \nu(\alpha) \geq 0\},$$

*and in this context we call A the **valuation ring of K** , denoted by $\mathcal{O}_K$.*

The following is the central example of a discrete valuation:

Definition D.4.4. Let $\alpha = (\alpha_1, \alpha_2, \dots) \in \mathbb{Z}_p$. The **p -adic valuation of α** , denoted by $\nu_p(\alpha)$, is the largest power of p which divides α . In other words, $\nu_p(\alpha)$ is the largest index i such that the component α_i is congruent to 0 modulo p^i . By convention, we define $\nu_p(0) := \infty$.

We extend ν_p to $\mathbb{Q}_p$ as described in Proposition D.4.5. In other words, for $\alpha \in \mathbb{Q}_p$, write $\alpha = \frac{\beta}{\gamma}$ for $\beta \in \mathbb{Z}_p$ and $\gamma \in \mathbb{Z}_p \setminus \{0\}$. Then $\nu_p(\alpha) := \nu_p(\beta) - \nu_p(\gamma)$.

Note in this case that $\mathbb{Z}_p$ is the valuation ring of $\mathbb{Q}_p$, i.e., $\mathbb{Z}_p = \mathcal{O}_{\mathbb{Q}_p}$, and that the value group of ν_p is simply $\mathbb{Z}$.

Example D.4.4. For $p = 2$, we have $\nu_2(8) = \nu_2(24) = 3$, $\nu_2(-6) = \nu_2(2) = 1$, and $\nu_2(24-8) = \nu_2(16) = 4$. On $\mathbb{Q}_2$, we have $\nu_2\left(\frac{9}{4}\right) = -2$. Compare this with, say, $\nu_2(24) = 3$.

One should think of ν_p as measuring the divisibility of a p -adic number by p . As in Example D.4.3, it will aid intuition to think of highly divisible p -adic integers as being small, hence the following definition:

Definition D.4.5. Let K be a field with a discrete valuation ν , and let $0 < c < 1$ be a real number. The **discrete absolute value associated with ν and c** , denoted by $|\cdot|_\nu$, is defined by $|\alpha|_\nu := c^{\nu(\alpha)}$ for all $\alpha \in K$.

By definition and by the properties of ν , such an absolute value has the following properties for all $\alpha, \beta \in K$:

1. $|\alpha|_\nu \geq 0$.
2. $|\alpha|_\nu = 0 \iff \alpha = 0$.
3. $|\alpha\beta|_\nu = |\alpha|_\nu |\beta|_\nu$.
4. $|\alpha + \beta|_\nu \leq \max\{|\alpha|_\nu, |\beta|_\nu\}$.

For such a field K and absolute value $|\cdot|_\nu$, we will always consider K as a topological space under the induced topology. That is, a subset $U \subseteq K$ is open if and only if, for any $\alpha \in U$, there exists $\varepsilon \in \mathbb{R}_{>0}$ such that the ball

$$B(\alpha, \varepsilon) := \{\beta \in K : |\alpha - \beta|_\nu < \varepsilon\}$$

is contained in U . Note that the above properties of $|\cdot|_\nu$ turn K into a topological field, and that different choices of the constant c define homeomorphic topologies.

Also note that in this case, the valuation ring $\mathcal{O}_K$ of K is given by

$$\mathcal{O}_K = \{\alpha \in K : |\alpha|_\nu \leq 1\}.$$

Note that, if $|\cdot|_1$ and $|\cdot|_2$ are two discrete absolute values on K for which there exists a real number $t > 0$ such that $|\cdot|_1 = |\cdot|_2^t$, then the resulting topologies on K are homeomorphic. In fact, this characterises the possibility of homeomorphic topologies arising from discrete absolute values. In this case, we call $|\cdot|_1$ and $|\cdot|_2$ **equivalent**.

In the special case of $A = \mathbb{Z}_p$ and $\nu = \nu_p$, we always choose $c = \frac{1}{p}$. The resulting absolute value is called the **p -adic absolute value** and is denoted by $|\cdot|_p$; explicitly, for $\alpha \in \mathbb{Q}_p$, we have

$$|\alpha|_p := p^{-\nu_p(\alpha)}.$$

As mentioned within the definition, choosing different bases of the exponent for the p -adic absolute value does not change the topology; it is a matter of convenience and convention.

Example D.4.5. Translating Example D.4.4, we have $|8|_2 = |24|_2 = \frac{1}{8}$, $|-6|_2 = |2|_2 = \frac{1}{2}$, and $|24 - 8|_2 = |16|_2 = \frac{1}{16}$. Intuitively, we see that 24 and 8 are rather 2-adically close together and that 8 and 24 are 2-adically smaller, i.e., closer to 0, than 2 and -6 . Further, $|\frac{9}{4}|_2 = 4$ while $|24|_2 = \frac{1}{8}$, so $\frac{9}{4}$ is 2-adically larger than 24.

Example D.4.6. Let $p = 2$ and consider the 2-adic integer

$$\beta = (1, 1, 5, 5, 21, 53, 53, \dots).$$

The given components of β have the following curious property:

$$\beta^2 + 7 = (8, 8, 32, 32, 448, 2816, 2816, \dots) = (0, 0, 0, 0, 0, 0, 0, \dots).$$

One can show with Hensel's Lemma, Theorem 1.2.1 or Lemma D.6.1, that this sequence can be 2-adically continued indefinitely. Thus, $\mathbb{Z}_2$ has a root of the polynomial $x^2 + 7$, which is irreducible over $\mathbb{Z}$. It is trickier to show that $x^2 - 7$ does not have a root in $\mathbb{Z}_2$, so $\mathbb{Z}_2$ (and its field of fractions, $\mathbb{Q}_2$, introduced in Section 1.5) is not algebraically closed.

Clearly $\nu_2(\beta) = 0$, so $|\beta|_2 = 1$. We have the following sequence of related integers:

$$\beta_1 = (1, 1, 1, 1, \dots)$$

$$\beta_2 = (1, 1, 5, 5, 5, 5, \dots)$$

$$\beta_3 = (1, 1, 5, 5, 21, 21, 21, \dots)$$

$$\beta_4 = (1, 1, 5, 5, 21, 53, 53, 53, 53, \dots).$$

Clearly, they are the integers 1, 5, 21, and 53, respectively. The corresponding sequence of 2-adic distances to β is

$$|\beta - \beta_1|_2 = |(0, 0, 4, 4, 20, 52, 52, \dots)|_2 = 2^{-2} = \frac{1}{4},$$

$$|\beta - \beta_2|_2 = |(0, 0, 0, 0, 4, 4, 16, 48, 48, \dots)|_2 = 2^{-4} = \frac{1}{16},$$

$$|\beta - \beta_3|_2 = \frac{1}{32},$$

$$|\beta - \beta_4|_2 = \frac{1}{256}.$$

Therefore, it is fair to refer to the β_j as 2-adic approximations of β . A similar procedure can be carried out in general, since $\mathbb{Z}$ is actually dense in $\mathbb{Z}_p$; see Proposition D.4.6.

The interactions between the algebra and topology of $\mathbb{Q}_p$ and $\mathbb{Z}_p$ are very rich and is responsible for the capstone theorem of this section.

Proposition D.4.6. [15, Lecture 8, Theorem 8.1] Equip $\mathbb{Q}_p$ with the metric topology defined by $|\cdot|_p$, and equip $\mathbb{Z}_p$ with the subspace topology. Then $\mathbb{Q}_p$ is a complete, Hausdorff, topological field, and $\mathbb{Q}$ is a dense subfield of $\mathbb{Q}_p$. In fact, $\mathbb{Q}_p$ is the metric completion of $\mathbb{Q}$. Moreover, $\mathbb{Z}_p$ is a compact (hence complete), Hausdorff, topological ring, $\mathbb{Z}$ is a dense subring, and $\mathbb{Z}_p$ is the metric completion of $\mathbb{Z}$.

In fact, the *only* metric completions of $\mathbb{Q}$ are $\mathbb{R}$ and $\mathbb{Q}_p$ for various primes p , up to a suitable notion of isomorphism. This is an easy consequence of the celebrated Ostrowski's Theorem ([15, Lecture 5, Theorem 5.6]).

Example D.4.7. Let $\alpha \in \mathbb{Z}_p$. Then obviously, for any $k \geq 1$, the ball

$$B_k(\alpha) := B(\alpha, p^{-k}) = \{y \in \mathbb{Z}_p : |\alpha - y|_p < p^{-k}\}$$

is open in $\mathbb{Z}_p$. But we can re-write this set in an interesting form:

$$\begin{aligned} B_k(\alpha) &= \{y \in \mathbb{Z}_p : \nu_p(\alpha - y) > k\} \\ &= \{(y_1, y_2, \dots) \in \mathbb{Z}_p : \alpha_i \equiv y_i \pmod{p^i} \text{ for all } 1 \leq i \leq k\} \\ &= \{(y_1, y_2, \dots) \in \mathbb{Z}_p : \alpha - y = (0, 0, 0, \dots, 0, \alpha_{k+1} - y_{k+1}, \alpha_{k+2} - y_{k+2}, \dots)\}. \end{aligned}$$

For the same $\alpha \in \mathbb{Z}_p$ and $k \geq 1$, the coset $\alpha + p^k \mathbb{Z}_p$ consists of exactly those p -adic integers whose difference with α is divisible by p^k . Thus, $B_k(\alpha) = \alpha + p^k \mathbb{Z}_p$.

In fact, using this observation and Corollary D.4.1, one can show that the complement $\mathbb{Z}_p \setminus B_k(\alpha)$ is also open, hence the ball $B_k(\alpha)$ is closed in $\mathbb{Z}_p$. Of course, as a closed subset of a compact space, $B_k(\alpha)$ is also compact.

Example D.4.8. Let $\varphi : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ be continuous, and for $k \geq 1$, let $S_k := \{\alpha \in \mathbb{Z}_p : \varphi(\alpha) \in p^k \mathbb{Z}_p\}$. Then S_k is closed; in fact, $S_k = \varphi^{-1}(p^k \mathbb{Z}_p)$, and $p^k \mathbb{Z}_p$ is the closed ball $B_k(0)$ (see Example D.4.7).

We are almost prepared to prove the main result of this section.

Lemma D.4.1. *For any prime p , the intersection*

$$\bigcap_{n \geq 1} p^n \mathbb{Z}_p$$

is $\{0\}$.

Proof. Let $\alpha \in \bigcap_{n \geq 1} p^n \mathbb{Z}_p$. If $\alpha \neq 0$, then $\nu_p(\alpha)$ is a non-negative integer which is larger than all $n \geq 1$, a contradiction. Thus $\alpha = 0$. $\square$

Theorem D.4.1. *Let $f(x) \in \mathbb{Z}[x]$ and for $n \geq 1$, let $\overline{f_n} \in \mathbb{Z}/p^n \mathbb{Z}[x]$ be the polynomial formed by reducing the coefficients of f modulo p^n . Then f has a root in $\mathbb{Z}_p$ if and only if $\overline{f_n}$ has a root for all $n \geq 1$.*

Proof. The forward direction is easy: If $\alpha \in \mathbb{Z}_p$ is a root of f , we can write $\alpha = (\alpha_1, \alpha_2, \dots)$. For $n \geq 1$, applying the canonical projection map $\pi_n : \mathbb{Z}_p \rightarrow \mathbb{Z}/p^n \mathbb{Z}$ to the $\mathbb{Z}_p$ -equation $f(\alpha) = 0$ gives the $\mathbb{Z}/p^n \mathbb{Z}$ -equation

$$\overline{f_n}(\pi_n(\alpha)) = \overline{f_n}(\alpha_n) = 0.$$

Thus $\overline{f_n}$ has a root given by the n^{th} component of the p -adic root α .

The proof of the converse uses compactness of $\mathbb{Z}_p$. We will prove non-constructively that there exists a p -adic root of f which is a limit of the roots of the $\overline{f_n}$.

Formally, consider the evaluation map $\text{ev}_f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, which is continuous since $\mathbb{Z}_p$ is a topological ring. As in Example D.4.8, let

$$S_n := \text{ev}_f^{-1}(p^n \mathbb{Z}_p) = \{\alpha \in \mathbb{Z}_p : f(\alpha) \in p^n \mathbb{Z}_p\},$$

which is closed, hence compact, in $\mathbb{Z}_p$.

Each S_n is non-empty, as if $\alpha_n \in \mathbb{Z}/p^n \mathbb{Z}$ is a root of $\overline{f_n}$, then any lift of α_n under π_n will be in S_n . Further, compatibility of sequences in $\mathbb{Z}_p$ implies that the S_n are nested, i.e., $S_{n+1} \subseteq S_n$ for all $n \geq 1$.

Thus, by compactness of $\mathbb{Z}_p$, the intersection $S := \bigcap_{n \geq 1} S_n$ is non-empty. Any $\alpha \in S$ has the property that $f(\alpha) \in \bigcap_{n \geq 1} p^n \mathbb{Z}_p$, so by Lemma D.4.1, $f(\alpha) = 0$. Thus α is a p -adic root of f . $\square$

We also have the following important consequence of Lemma D.4.1, which has the dual purposes of justifying the earlier statement regarding the simplicity of the algebra of $\mathbb{Z}_p$, and re-contextualising the p -adic valuation ν_p :

Corollary D.4.2. [15, Lecture 4, Theorems 4.15 and 4.16] Every non-zero, proper ideal of the p -adic integers $\mathbb{Z}_p$ is of the form $p^k\mathbb{Z}_p$ for some $k \geq 1$. Further, in light of Proposition D.4.4, any non-zero $\alpha \in \mathbb{Z}_p$ can be written in the form $\alpha = p^k u$, where $k \geq 1$ and $u \in \mathbb{Z}_p$ is invertible, and in this notation, $\nu_p(\alpha) = k$.

D.5 Finite Extensions of $\mathbb{Q}_p$

The goal of this section is to explain why the degree of a finite extension of the p -adic numbers $\mathbb{Q}_p$ is the product of the ramification and inertia degrees of the extension.

Intuitively, this result holds because there are two defining features of $\mathbb{Q}_p$, namely, the valuation ν_p and the residue field $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$; thus, to extend $\mathbb{Q}_p$ we can independently extend ν_p or extend the finite field $\mathbb{F}_p$, and this gives all information about the entire extension.

One should draw many comparisons with Section D.1, which highlights the remarkably simple algebraic properties of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ compared with $\mathbb{Z}$ and $\mathbb{Q}$.

Note that $\mathbb{Q}_p$ fits into a larger family of topological fields called *local fields*. Most results from this section hold for finite extensions of other local fields, but we will eschew this further generality in favour of brevity.

The primary reference for this section is Chapter II, Section 3 of Neukirch's text ([52]).

We start with the following non-standard terminology:

Definition D.5.1. Let $p \in \mathbb{Z}$ be prime. A **p -adic field** is a finite extension $\widehat{L}$ of the p -adic numbers $\mathbb{Q}_p$, equipped with a discrete absolute value $|\cdot|_{\widehat{L}}$ (see Definitions D.4.3 and D.4.5) which extends the p -adic absolute value $|\cdot|_p$ in the sense that $|\alpha|_{\widehat{L}} = |\alpha|_p$ for all $\alpha \in \mathbb{Q}_p$. Note that we always consider $\widehat{L}$ as a topological field with the metric topology induced by $|\cdot|_{\widehat{L}}$.

Example D.5.1. We saw in Example D.4.6 that $\mathbb{Q}_2$ contains an element which deserves the name $\sqrt{-7}$, i.e., a root of $x^2 + 7 \in \mathbb{Q}_2[x]$. One can show with valuations, however, that there is no element that could reasonably be called $\sqrt{2}$, i.e., there is no root of $x^2 - 2$ in $\mathbb{Q}_2$. Thus, we can form the extension $\mathbb{Q}_2(\sqrt{2}) \cong \mathbb{Q}_2[x]/\langle x^2 - 2 \rangle$, which is of degree 2 and has basis $\{1, \sqrt{2}\}$ over $\mathbb{Q}_2$.

Note that $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$ is Galois, and for $\alpha = a + b\sqrt{2} \in \mathbb{Q}_2(\sqrt{2})$ (for $a, b \in \mathbb{Q}_2$), the **Galois conjugate of α in $\mathbb{Q}_2(\sqrt{2})$** is $\bar{\alpha} := a - b\sqrt{2}$, and the **norm of α in $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$** is $N(\alpha) := \alpha\bar{\alpha} = a^2 - 2b^2$ (see Definition D.2.2 in Section D.2). We use this to define an

absolute value on $\mathbb{Q}_2(\sqrt{2})$ by $|\alpha| := \sqrt{|\alpha\bar{\alpha}|_2} = \sqrt{|a^2 - 2b^2|_2}$. It is straightforward to check that this turns $\mathbb{Q}_2$ into a 2-adic field, i.e., that $|\cdot|$ is a discrete absolute value which extends $|\cdot|_2$.

As a concrete example, we have $|\sqrt{2}| = \sqrt{|-2|_2} = \sqrt{\frac{1}{2}}$, while $|2| = \sqrt{|2^2|_2} = \sqrt{2^{-2}} = \frac{1}{2}$. In particular, notice that $\sqrt{2}$ is smaller than 2 in $\mathbb{Q}_2(\sqrt{2})$, yet 2 has the smallest possible absolute value in $\mathbb{Q}_2$.

Recall that a field K equipped with a discrete absolute value has a distinguished subring called the *valuation ring*, defined as

$$\mathcal{O}_K := \{\alpha \in K : |\alpha| \leq 1\}.$$

The following is a generalisation of Proposition D.4.4:

Proposition D.5.1. [52, Chapter II, Propositions 3.8 and 3.9] Let $\widehat{L}/\mathbb{Q}$ be a p -adic field with absolute value $|\cdot|_{\widehat{L}}$. Then the set of non-units of $\mathcal{O}_{\widehat{L}}$ is

$$\mathfrak{p}_{\widehat{L}} = \{\alpha \in K : |\alpha|_{\widehat{L}} < 1\},$$

and moreover, $\mathfrak{p}_{\widehat{L}}$ is principal. In particular, $\mathcal{O}_{\widehat{L}}$ is a local ring.

Example D.5.2. Continuing Example D.5.1, let $\mathcal{O}$ and $\mathfrak{p}$ denote the valuation ring and maximal ideal, respectively, of $\mathbb{Q}_2(\sqrt{2})$. We saw previously that $|\sqrt{2}| = \sqrt{\frac{1}{2}} < 1$, so $\sqrt{2} \in \mathfrak{p}$. Further, let $a, b \in \mathbb{Z}_2$, so that $|a| = |a|_2 \leq 1$, and similarly for b . Then by the non-Archimedean property,

$$|a + b\sqrt{2}| \leq \max \left\{ |a|, |\sqrt{2}| \cdot |b| \right\} \leq 1.$$

Thus $\mathbb{Z}_2[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}_2\} \subseteq \mathcal{O}$. The other inclusion can be proved using the trace and norm functions on the extension $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$.

In fact, similar ideas can prove that $\sqrt{2}$ is a generator of $\mathfrak{p}$. Indeed, first note that the extension $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$ is Galois, since the roots of $x^2 - 2 \in \mathbb{Q}_2[x]$ are $\pm\sqrt{2}$. The non-trivial element of $G := \text{Gal}(\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2)$ is $a + b\sqrt{2} \mapsto a - b\sqrt{2}$, and note that this preserves $|\cdot|$, i.e., $|a + b\sqrt{2}| = |a - b\sqrt{2}|$. Thus, for $\alpha = a + b\sqrt{2} \in \mathbb{Q}_2(\sqrt{2})^\times$ with Galois conjugate $\bar{\alpha} = a - b\sqrt{2}$,

$$|N(\alpha)| = |\alpha\bar{\alpha}| = |\alpha|^2.$$

But $N(\alpha) \in \mathbb{Q}_2^\times$ by norm properties, so there is some $n \in \mathbb{Z}$ such that $|N(\alpha)| = 2^{-n}$. Thus, for $\alpha \in \mathbb{Q}_2(\sqrt{2})^\times$ there is $n \in \mathbb{Z}$ such that $|\alpha| = 2^{-n/2}$.

Taking the corresponding discrete valuation as $\nu(\alpha) := -\log_2(|\alpha|)$ for $\alpha \in \mathbb{Q}_2(\sqrt{2})$ (i.e., implicitly choosing the constant $\frac{1}{2}$ in Definition D.4.5), the above shows that the value group of $\mathbb{Q}_2(\sqrt{2})$ is $\frac{1}{2}\mathbb{Z}$. In particular, $\sqrt{2}$ has the smallest possible positive valuation of $\frac{1}{2}$.

From here, it is simple to prove the claim that $\mathfrak{p} = \langle \sqrt{2} \rangle$ in $\mathcal{O}$.

Example D.5.3. One can show that $x^3 - x - 1 \in \mathbb{Q}_3[x]$ is irreducible; if θ is a root (living in some algebraic closure of $\mathbb{Q}_3$), then $\mathbb{Q}_3(\theta)/\mathbb{Q}_3$ is a 3-adic field of degree 3. Omitting the details this time, one can prove that the valuation ring $\mathcal{O}$ is $\mathbb{Z}_3[\theta] := \{a + b\theta + c\theta^2 : a, b, c \in \mathbb{Z}_3\}$ and the maximal ideal $\mathfrak{p}$ is $\langle 3 \rangle$; the last fact follows after observing that this extension is cyclic, and 3 has the minimal positive valuation. In particular, 3 and θ do not differ by a unit-multiple in $\mathcal{O}$, so θ is **not** a generator of $\mathfrak{p}$.

From Proposition D.5.1 and the properties of discrete valuations, we have the following wonderful result:

Corollary D.5.1. [52, Chapter II, Proposition 3.9] Let $\widehat{L}/\mathbb{Q}_p$ be a p -adic field. Then every non-zero, proper ideal of $\mathcal{O}_{\widehat{L}}$ is a power of the unique maximal ideal $\mathfrak{p}_{\widehat{L}}$. In particular, if $\mathfrak{p}_{\widehat{L}} = \langle \pi_{\widehat{L}} \rangle$ for some $\pi_{\widehat{L}} \in \mathcal{O}_{\widehat{L}}$, then for every $\alpha \in \mathcal{O}_{\widehat{L}}$, there exists a unit $u \in \mathcal{O}_{\widehat{L}}^\times$ and a unique integer $k \geq 0$ such that $\alpha = \pi_{\widehat{L}}^k u$.

Of course, then, generators of maximal ideals of valuation rings are very important:

Definition D.5.2. Let $\widehat{L}/\mathbb{Q}_p$ be a p -adic field. A **uniformiser** or **uniformising element** of $\widehat{L}$ is a generator of the unique maximal ideal $\mathfrak{p}_{\widehat{L}}$ of $\mathcal{O}_{\widehat{L}}$. Note that any two uniformisers of $\widehat{L}$ differ by a unit-multiple in $\mathcal{O}_{\widehat{L}}$.

Example D.5.4. As a consequence of Proposition D.4.4, a uniformiser of $\mathbb{Q}_p$ itself is p .

We saw in Example D.5.2 that $\sqrt{2}$ is a uniformiser of the 2-adic field $\mathbb{Q}_2(\sqrt{2})$, and in Example D.5.3 that 3 is a uniformiser of the 3-adic field $\mathbb{Q}_3(\theta)$, where θ is a root of $x^3 - x - 1$.

For reasons that will become apparent soon, we point out that in $\mathbb{Q}_2(\sqrt{2})$, $\langle 2 \rangle = \langle \sqrt{2} \rangle^2$, and in $\mathbb{Q}_3(\theta)$, $\langle 3 \rangle$ is the maximal ideal of the valuation ring.

The following connects the topology of p -adic fields and their valuation rings with their algebra, and is also a p -adic analogue of Proposition D.1.1:

Proposition D.5.2. [52, Chapter II, Proposition 5.1] Let $\widehat{L}/\mathbb{Q}_p$ be a p -adic field of degree n . Then the valuation ring $\mathcal{O}_{\widehat{L}}$ is a compact subring of $\widehat{L}$ which is also a free $\mathbb{Z}_p$ -module of rank n .

Every local ring has a canonically associated field, and this is of particular importance for p -adic fields:

Definition D.5.3. Let $\widehat{L}/\mathbb{Q}$ be a p -adic field with uniformiser $\pi_{\widehat{L}}$. The **residue field of $\widehat{L}$** , denoted by $\kappa_{\widehat{L}}$, is the quotient $\mathcal{O}_{\widehat{L}}/\langle\pi_{\widehat{L}}\rangle$.

Example D.5.5. By Corollary D.4.1, the residue field of $\mathbb{Q}_p$ is $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

We are able to give more interesting examples with the following result, which follows from Corollary D.4.1 and Proposition D.5.2:

Proposition D.5.3. Let $\widehat{L}/\mathbb{Q}_p$ be a p -adic field. Then the residue field $\kappa_{\widehat{L}}$ is a finite extension of $\mathbb{F}_p$.

Example D.5.6. We saw in Example D.5.2 that $\mathcal{O}_{\mathbb{Q}_2(\sqrt{2})} = \mathbb{Z}_2[\sqrt{2}]$ and that $\sqrt{2}$ is a uniformiser; it is simple to show that there are exactly two classes in $\mathbb{Z}_2[\sqrt{2}]/\langle\sqrt{2}\rangle$, so $\kappa_{\mathbb{Q}_2(\sqrt{2})} \cong \mathbb{F}_2$.

In Example D.5.3, we described a cubic 3-adic field $\mathbb{Q}_3(\theta)$ with valuation ring $\mathbb{Z}_3[\theta]$ and uniformiser 3. One can show that the defining polynomial $x^3 - x - 1 \in \mathbb{Q}_3[x]$ remains irreducible over $\mathbb{F}_3$, meaning that the images of the $\mathbb{Z}_3$ -basis $\{1, \theta, \theta^2\}$ of $\mathbb{Z}_3[\theta]$ reduce to an $\mathbb{F}_3$ -basis of the residue field $\kappa_{\mathbb{Q}_3(\theta)}$. In particular, $\kappa_{\mathbb{Q}_3(\theta)} \cong \mathbb{F}_{3^3}$.

Now we define two important numerical quantities associated with p -adic fields. The names will be familiar from Definitions D.1.5 and D.1.6:

Definition D.5.4. Let $\widehat{L}/\mathbb{Q}_p$ be a p -adic field of degree n with uniformiser $\pi_{\widehat{L}}$. The **ramification degree of $\widehat{L}$** , denoted by $e_{\widehat{L}}$, is the positive integer such that $p\mathcal{O}_{\widehat{L}} = \langle\pi_{\widehat{L}}\rangle^{e_{\widehat{L}}}$. The **inertia degree** or **residue class degree of $\widehat{L}$** , denoted by $f_{\widehat{L}}$, is the degree of the residue field extension $[\kappa_{\widehat{L}} : \mathbb{F}_p]$. If $e_{\widehat{L}} = 1$, then we call $\widehat{L}/\mathbb{Q}_p$ **unramified**. On the other hand, if $e_{\widehat{L}} = n$, then $\widehat{L}/\mathbb{Q}_p$ is called **totally ramified**.

Example D.5.7. Example D.5.4 shows that $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$ is totally ramified and that $\mathbb{Q}_3(\theta)$ is unramified.

The similarities do not end with the nomenclature: We will see in Section D.6 that each p -adic field corresponds to the completion of a number field at a prime above the rational prime p , and the ramification and inertia degrees of that prime in the number field setting are exactly the ones in the corresponding p -adic setting.

In the meantime, we will finish this section by proving a p -adic analogue of Proposition D.1.6. First we recall a form Nakayama's Lemma for local rings from commutative algebra:

Lemma D.5.1. *[2, Proposition 2.8] Let A be a local ring with maximal ideal $\mathfrak{m}$, and let M be a finitely generated A -module. If $\overline{\mathcal{B}} := \{b_1 + \mathfrak{m}M, \dots, b_r + \mathfrak{m}M\}$ is an $(A/\mathfrak{m})$ -basis of $M/\mathfrak{m}M$ as a vector space, then $\mathcal{B} := \{b_1, \dots, b_r\}$ is a minimal generating set of M as an A -module.*

Theorem D.5.1. *Let $\widehat{L}/\mathbb{Q}$ be a p -adic field of degree n with ramification degree $e_{\widehat{L}}$ and inertia degree $f_{\widehat{L}}$. Then $n = e_{\widehat{L}}f_{\widehat{L}}$.*

Proof. Let $\pi_{\widehat{L}}$ be a uniformiser of $\widehat{L}$. By definition, $p\mathcal{O}_{\widehat{L}} = \langle \pi_{\widehat{L}} \rangle^{e_{\widehat{L}}}$, so we have the filtration

$$\mathcal{O}_{\widehat{L}} \supseteq \langle \pi_{\widehat{L}} \rangle \supseteq \langle \pi_{\widehat{L}} \rangle^2 \supseteq \dots \supseteq \langle \pi_{\widehat{L}} \rangle^{e_{\widehat{L}}-1} \supseteq \langle \pi_{\widehat{L}} \rangle^{e_{\widehat{L}}} = p\mathcal{O}_{\widehat{L}}, \quad (\text{D.2})$$

and the successive quotients are

$$\langle \pi_{\widehat{L}} \rangle^j / \langle \pi_{\widehat{L}} \rangle^{j+1}, \quad 0 \leq j \leq e_{\widehat{L}} - 1.$$

For each j , the multiplication-by- $\pi_{\widehat{L}}^j$ map induces an isomorphism of $\mathcal{O}_{\widehat{L}}/\langle \pi_{\widehat{L}} \rangle$ -modules

$$\mathcal{O}_{\widehat{L}}/\langle \pi_{\widehat{L}} \rangle \rightarrow \langle \pi_{\widehat{L}} \rangle^j / \langle \pi_{\widehat{L}} \rangle^{j+1},$$

so each $\langle \pi_{\widehat{L}} \rangle^j / \langle \pi_{\widehat{L}} \rangle^{j+1}$ is isomorphic as an $\mathbb{F}_p$ -vector space to the residue field $\mathcal{O}_{\widehat{L}}/\langle \pi_{\widehat{L}} \rangle = \kappa_{\widehat{L}}$. By definition, $\kappa_{\widehat{L}}$ has dimension $f_{\widehat{L}}$ over $\mathbb{F}_p$.

Now we use the filtration (1.2) to build a direct sum decomposition of $\mathcal{O}_{\widehat{L}}/p\mathcal{O}_{\widehat{L}} = \mathcal{O}_{\widehat{L}}/\langle \pi_{\widehat{L}} \rangle^{e_{\widehat{L}}}$. Indeed, the map

$$\mathcal{O}_{\widehat{L}}/p\mathcal{O}_{\widehat{L}} \rightarrow \bigoplus_{j=0}^{e_{\widehat{L}}-1} \langle \pi_{\widehat{L}} \rangle^j / \langle \pi_{\widehat{L}} \rangle^{j+1},$$

$$\alpha + p\mathcal{O}_{\widehat{L}} \mapsto (\alpha + \langle \pi_{\widehat{L}} \rangle, \alpha + \langle \pi_{\widehat{L}} \rangle^2, \dots, \alpha + \langle \pi_{\widehat{L}} \rangle^{e_{\widehat{L}}})$$

can be shown to be an isomorphism of $\mathbb{F}_p$ -vector spaces (surjectivity is the trickiest part, but one can build a lift of a residue class inductively on j). Thus $\mathcal{O}_{\widehat{L}}/p\mathcal{O}_{\widehat{L}}$ has dimension $e_{\widehat{L}}f_{\widehat{L}}$ as an $\mathbb{F}_p$ -vector space.

Let $b_1, \dots, b_f \in \mathcal{O}_{\widehat{L}}$ be elements whose residue classes $\overline{\mathcal{B}} := \{b_1 + \langle \pi_{\widehat{L}} \rangle, \dots, b_f + \langle \pi_{\widehat{L}} \rangle\}$ in $\mathcal{O}_{\widehat{L}}/\langle \pi_{\widehat{L}} \rangle$ form an $\mathbb{F}_p$ -basis. For each j , $0 \leq j \leq e_{\widehat{L}} - 1$, $\{b_1 \pi_{\widehat{L}}^j, \dots, b_f \pi_{\widehat{L}}^j\}$ descends to an $\mathbb{F}_p$ -basis of $\langle \pi_{\widehat{L}} \rangle^j / \langle \pi_{\widehat{L}} \rangle^{j+1}$ via the multiplication-by- $\pi_{\widehat{L}}^j$ map. Collecting over all such j shows that $\{b_i \pi_{\widehat{L}}^j + \langle \pi_{\widehat{L}} \rangle^{j+1} : 1 \leq i \leq f, 0 \leq j \leq e_{\widehat{L}} - 1\}$ is an $\mathbb{F}_p$ -basis of $\mathcal{O}_{\widehat{L}}/p\mathcal{O}_{\widehat{L}}$.

Finally, by Nakayama's Lemma D.5.1, $\{b_i \pi_{\widehat{L}}^j : i \leq 1 \leq f_{\widehat{L}}, 0 \leq j \leq e_{\widehat{L}} - 1\}$ is a minimal generating set of $\mathcal{O}_{\widehat{L}}$ as a $\mathbb{Z}_p$ -module, and since $\mathcal{O}_{\widehat{L}}$ is free as a $\mathbb{Z}_p$ -module, this minimal generating set is a $\mathbb{Z}_p$ -basis for $\mathcal{O}_{\widehat{L}}$. As $\mathcal{O}_{\widehat{L}}$ has rank n over $\mathbb{Z}_p$, this finishes the proof. $\square$

D.6 Extensions of the p -Adic Absolute Value

The goal of this final background section is to explain why every p -adic field arises as the completion of a number field at a prime $\mathfrak{p}$ above p , and the consequent connections to polynomial factorisations, which will be used in Section 2.1.

More specifically, we explore discrete absolute values on number fields, and how they are viewed as extensions of the p -adic absolute values on $\mathbb{Q}$ and $\mathbb{Q}_p$. This section provides yet more contrast between number fields and p -adic fields.

Definition D.6.1. Let $L/\mathbb{Q}$ be a number field and $\mathfrak{p}$ be a prime of L . Let p be the rational prime lying below $\mathfrak{p}$, and e be the ramification degree of $\mathfrak{p}$ above p . For $\alpha \in \mathcal{O}_L$, the **$\mathfrak{p}$ -adic valuation** of α , denoted by $\nu_{\mathfrak{p}}(\alpha)$, is defined as $\frac{1}{e}$ times the exponent of $\mathfrak{p}$ in the unique prime ideal factorisation of the principal ideal $\alpha\mathcal{O}_L$. By convention, we define $\nu_{\mathfrak{p}}(0) := \infty$.

Since L is the field of fractions of $\mathcal{O}_L$, we can extend $\nu_{\mathfrak{p}}$ to L as described in Proposition D.4.5. Explicitly, write $\alpha \in L$ as $\alpha = \frac{\beta}{\gamma}$ for $\beta, \gamma \in \mathcal{O}_L$ and $\gamma \neq 0$. Then we define $\nu_{\mathfrak{p}}(\alpha) := \nu_{\mathfrak{p}}(\beta) - \nu_{\mathfrak{p}}(\gamma)$.

Of course, this defines a discrete valuation on L and $\mathcal{O}_L$ with value group $\frac{1}{e}\mathbb{Z}$. We can also define the **$\mathfrak{p}$ -adic absolute value** on L by $|\cdot|_{\mathfrak{p}} := p^{-\nu_{\mathfrak{p}}(\cdot)}$, i.e., by choosing $c = \frac{1}{p}$ in Definition D.4.5.

As expected, the resulting topology turns L into a topological field, with $\mathcal{O}_L$ as a compact topological subring characterised by

$$\mathcal{O}_L = \{\alpha \in L : \nu_{\mathfrak{p}}(\alpha) \geq 0\} = \{\alpha \in L : |\alpha|_{\mathfrak{p}} \leq 1\}.$$

The choice of constants $\frac{1}{e}$ and $c = \frac{1}{p}$ guarantees that $|\cdot|_{\mathfrak{p}}$ extends $|\cdot|_p$ on $\mathbb{Q}$; for example, by definition of the ramification degree, $\nu_{\mathfrak{p}}(p) = \frac{1}{e}e = 1 = \nu_p(p)$.

The situation with inequivalent discrete valuations on number fields is very similar to $\mathbb{Q}$ itself: There is exactly one for each prime. This is *Ostrowski's Theorem for Number Fields* ([21, Theorem 3]).

Example D.6.1. From Example D.1.5, some possible valuations on the Gaussian numbers $\mathbb{Q}(i)$ are with respect to $\mathfrak{p}_1 := \langle 2+3i \rangle$, $\mathfrak{p}_2 := \langle 2-3i \rangle$, and $\mathfrak{p}_3 := \langle 1+i \rangle$, whose corresponding ramification degrees are 1, 1, and 2. Then we have $\nu_{\mathfrak{p}_1}(13) = \nu_{\mathfrak{p}_2}(13) = 1$, $\nu_{\mathfrak{p}_3}(13) = 0$, and $\nu_{\mathfrak{p}_3}(2) = 1$. Thus $|13|_{\mathfrak{p}_1} = |13|_{\mathfrak{p}_2} = \frac{1}{13}$, $|13|_{\mathfrak{p}_3} = 1$, and $|2|_{\mathfrak{p}_3} = \frac{1}{2}$.

Importantly, note that $|\mathfrak{p}_1|_{\mathfrak{p}_1} = \frac{1}{13}$ and $|\mathfrak{p}_1|_{\mathfrak{p}_2} = 1$; in particular, there is no positive real number t such that $|\mathfrak{p}_1|_{\mathfrak{p}_1} = |\mathfrak{p}_1|_{\mathfrak{p}_2}^t$. As a consequence, $|\cdot|_{\mathfrak{p}_1}$ and $|\cdot|_{\mathfrak{p}_2}$ do **not** define homeomorphic topologies, i.e., are inequivalent, even though they both extend $|\cdot|_{13}$ on $\mathbb{Q}$.

The above example shows that choosing a different prime above p gives an inequivalent discrete absolute value which extends $|\cdot|_p$. Thus, one might expect the situation to simplify greatly when we move to p -adic fields, which only have one prime ideal. Confirming this is our next sub-goal. Indeed, we will now explain that every p -adic field arises as the completion of a number field at a discrete absolute value. The key step is Krasner's Lemma, which connects the algebra and topology of a field equipped with an absolute value.

Definition D.6.2. Let $p \in \mathbb{Z}$ be prime and let $\overline{\mathbb{Q}_p}$ be an algebraic closure of $\mathbb{Q}_p$. Finally, let $\theta, \theta' \in \overline{\mathbb{Q}_p}$. We say that θ' **belongs to** θ if $|\theta - \theta'|_p < |\sigma(\theta) - \theta'|_p$ for all non-identity embeddings $\sigma : \mathbb{Q}_p(\theta) \rightarrow \overline{\mathbb{Q}_p}$.

Embeddings $\mathbb{Q}_p(\theta) \rightarrow \overline{\mathbb{Q}_p}$ correspond to choosing a Galois conjugate of θ in $\mathbb{Q}_p(\theta)$, i.e., an element of $\mathbb{Q}_p(\theta)$ with the same minimal polynomial over $\mathbb{Q}_p$. In the Galois case, one can think of these as automorphisms in $\text{Gal}(\mathbb{Q}_p(\theta)/\mathbb{Q}_p)$.

Lemma D.6.1. [Krasner's Lemma [53, Lemma 8.1.6], [47, Proposition 7.60]] Let $\overline{\mathbb{Q}_p}$ be an algebraic closure of $\mathbb{Q}_p$ and $\theta, \theta' \in \overline{\mathbb{Q}_p}$. If θ' belongs to θ , then $K(\theta) \subseteq K(\theta')$.

Intuitively, Krasner's Lemma says that two elements which are algebraic over $\mathbb{Q}_p$ and are close enough to each other will define the same p -adic field.

A standard application of this result shows that every p -adic field arises as the completion of a number field:

Proposition D.6.1. [57, Corollary 3] Let $\widehat{L}/\mathbb{Q}_p$ be a p -adic field of degree n . Then there is a number field $L/\mathbb{Q}$ of degree n and a prime $\mathfrak{p}$ of L lying above p such that $\widehat{L}$ is the metric completion of L with respect to $|\cdot|_{\mathfrak{p}}$. Moreover, in this case, the valuation ring $\mathcal{O}_{\widehat{L}}$ is the metric completion of the ring of integers $\mathcal{O}_L$ with respect to $|\cdot|_{\mathfrak{p}}$. Further, the extended ideal $\mathfrak{p}\mathcal{O}_{\widehat{L}}$ is exactly the unique maximal ideal $\mathfrak{p}_{\widehat{L}}$ of $\mathcal{O}_{\widehat{L}}$.

This justifies the notation $\widehat{L}$ that we have used since Section D.5, as the hat symbol traditionally denotes the completion of some metric space.

By analysing a proof of Proposition D.6.1, it is straightforward to produce examples:

Example D.6.2. *One can show that $\mathbb{Q}_2$ does not contain a root of $x^2 + 1$, which we denote by i . In fact, $\mathbb{Q}_2(i)$ is the completion of the Gaussian numbers $\mathbb{Q}(i)$ with respect to the valuation defined by $\langle 1 + i \rangle$, which is the only prime of $\mathbb{Q}(i)$ above 2, and consequently, $\mathbb{Z}_2[i]$ is the completion of $\mathbb{Z}[i]$.*

We now have the language to explain why the ramification and inertia degrees defined for p -adic fields in Section D.5 agree with the corresponding notions for number fields from Section D.1.

Proposition D.6.2. *Let $\widehat{L}/\mathbb{Q}_p$ be a p -adic field arising as the completion of the number field $L/\mathbb{Q}$ with respect to the absolute value $|\cdot|_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime of L above p . Then $e_{\widehat{L}}$ is equal to the ramification degree $e_L(\mathfrak{p} \mid p)$, and $f_{\widehat{L}}$ is equal to the inertia degree $f_L(\mathfrak{p} \mid p)$.*

The intuitive reasoning is as follows: By definition of $e_L = e_L(\mathfrak{p} \mid p)$, we have the factorisation

$$p\mathcal{O}_L = \mathfrak{p}^{e_L} \prod_{i=2}^g \mathfrak{p}_i^{e_i}.$$

In the completion $\mathcal{O}_{\widehat{L}}$, for all i , every element of $\mathfrak{p}_i$ becomes a unit, hence the factorisation collapses to

$$p\mathcal{O}_{\widehat{L}} = \mathfrak{p}^{e_L} \mathcal{O}_{\widehat{L}}.$$

But $\mathfrak{p}\mathcal{O}_{\widehat{L}} = \langle \pi_{\widehat{L}} \rangle$, so $e_L = e_L(\mathfrak{p} \mid p) = e_{\widehat{L}}$.

For inertia degrees, one can use similar module-theoretic arguments as in the proof of Theorem D.5.1 to show that $\mathcal{O}_{\widehat{L}}/\langle \pi_{\widehat{L}} \rangle = \mathcal{O}_{\widehat{L}}/\mathfrak{p}\mathcal{O}_{\widehat{L}} \cong \mathcal{O}_L/\mathfrak{p}$, which is analogous to Corollary D.4.1.

We saw in Example D.6.1 that there may be inequivalent ways to extend the p -adic valuation from $\mathbb{Q}$ to a number field L . Our next sub-goal is to explain why this problem disappears for $\mathbb{Q}_p$ and p -adic fields.

The crucial puzzle piece is the following generalisation of Hensel's Lemma; see Theorem 1.2.1 for a more specialised version. The proof method is actually similar to that of Theorem D.5.1 in its reliance on commutative algebra results such as Nakayama's Lemma.

Theorem D.6.1 (Hensel's Lemma). *[52, Chapter II, Lemma 4.6] Let $\widehat{L}/\mathbb{Q}_p$ be a p -adic field with maximal ideal $\mathfrak{p}_{\widehat{L}}$ and residue field $\kappa_{\widehat{L}}$. Suppose that $f(x) \in \mathcal{O}_{\widehat{L}}[x]$ is primitive.*

Let $\bar{f}(x) \in \kappa_{\hat{L}}[x]$ denote the reduction of $f(x)$ modulo $\mathfrak{p}$, and suppose that $\bar{f}(x)$ factors as a product $g_0(x)h_0(x)$ of coprime polynomials in $\kappa_{\hat{L}}[x]$. Then there exist polynomials $g(x), h(x) \in \mathcal{O}_{\hat{L}}[x]$ such that $f(x) = g(x)h(x)$, $\bar{g}(x) = g_0(x)$ and $\bar{h}(x) = h_0(x)$, and $\deg(g) = \deg(g_0)$. Moreover, $g(x)$ and $h(x)$ are coprime in $\mathcal{O}_{\hat{L}}[x]$, and this factorisation of $f(x)$ is unique up to multiples of elements in $1 + \mathfrak{p}$.

Example D.6.3. Consider $f(x) := x^8 + x^2 + 1 \in \mathbb{Q}_{229}[x]$ (229 was chosen as it divides the polynomial discriminant). In $\mathbb{F}_{229}[x]$, we have the factorisation

$$x^8 + x^2 + 1 = (x + 103)^2(x + 126)^2(x^2 + 110x + 171)(x^2 + 119x + 171).$$

It is simple to show that these factors are coprime in $\mathbb{F}_{229}[x]$, so Hensel's Lemma lifts this to a product of 4 quadratics in $\mathbb{Z}_{229}[x]$.

This example also shows the necessity of the assumption that the residue field factorisation $\bar{f}(x) = g_0(x)h_0(x)$ is coprime: In $\mathbb{F}_2[x]$ (note, 2 is the other prime divisor of the polynomial discriminant), $x^8 + x^2 + 1$ factors as $(x^4 + x + 1)^2$, but it is straightforward to show that it cannot factor as a product of two quartics in $(\mathbb{Z}/4\mathbb{Z})[x]$, hence in $\mathbb{Z}_2[x]$.

Example D.6.4. For any prime p , $x^{p-1} - 1 \in \mathbb{Z}_p[x]$ factors as

$$(x - 1) \cdot (x - 2) \cdots (x - p + 1) \in \mathbb{F}_p[x],$$

so by Hensel's Lemma, it also splits completely into linear factors in $\mathbb{Z}_p[x]$. In other words, $\mathbb{Z}_p$ contains all possible $(p - 1)^{\text{st}}$ roots of unity.

Now one can show that there is exactly one extension of the p -adic absolute value from $\mathbb{Q}_p$ to a p -adic field:

Theorem D.6.2. [52, Chapter II, Theorem 4.8] Let $\hat{L}/\mathbb{Q}_p$ be a p -adic field of degree n . By Proposition D.6.1, view $\hat{L}$ as the completion of the number field L with respect to the discrete absolute value $|\cdot|_{\mathfrak{p}}$ defined by the prime $\mathfrak{p}$ lying above p . Then $|\cdot|_{\mathfrak{p}}$ is the unique absolute value extending $|\cdot|_p$ to $\hat{L}$, and moreover, an expression for $|\cdot|_{\mathfrak{p}}$ is

$$|\cdot|_{\mathfrak{p}} = \left| N_{\hat{L}/\mathbb{Q}_p}(\cdot) \right|_p^{1/n},$$

where $N_{\hat{L}/\mathbb{Q}_p}$ is the field norm defined for arbitrary finite extensions in Definition D.2.2.

Interestingly, the important application of Hensel's Lemma in the above is to show that if $\alpha \in \hat{L}$ is such that $N(\alpha) \in \mathbb{Z}_p$, then $\alpha \in \mathcal{O}_{\hat{L}}$. In other words, Hensel's Lemma implies a converse of Proposition D.2.2.

Example D.6.5. Recall the absolute value defined on $\mathbb{Q}_2(\sqrt{2})$ in Example D.5.1: For $\alpha := a + b\sqrt{2} \in \mathbb{Q}_2(\sqrt{2})$, let $\bar{\alpha} := a - b\sqrt{2}$. Then define $|\alpha| := \sqrt{|\alpha\bar{\alpha}|_2} = \sqrt{|a^2 - 2b^2|_2}$. Observing that $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$ is Galois as it contains both roots of $x^2 - 2 \in \mathbb{Q}_2[x]$, and α and $\bar{\alpha}$ are therefore Galois conjugates, this absolute value is exactly the one described in Theorem D.6.2.

To end this section, we prove a result connecting discrete absolute values on a number field with factorisations of its defining polynomial. We require two commutative algebra lemmas:

Lemma D.6.2. [24, Chapter 2, Proposition 2.5] Let L/K and M/K be two field extensions, with L/K being finite and separable. Then the map

$$L \rightarrow L \otimes_K M, \quad \alpha \mapsto \alpha \otimes_K 1$$

is an embedding of K -algebras.

Using the above notation and further assuming that we have a tower $M/L/K$ (not necessarily finite), there exists an irreducible $f(x) \in K[x]$ such that $L \cong K[x]/\langle f(x) \rangle$. Now suppose that $f(x)$ factors as $g_1(x) \cdots g_r(x)$ in $M[x]$. Then by the Chinese Remainder Theorem,

$$L \otimes_K M \cong K[x]/\langle f(x) \rangle \otimes_K M \cong M[x]/\langle f(x) \rangle \cong \prod_{i=1}^r M[x]/\langle g_i(x) \rangle.$$

Thus, we have proved the following:

Lemma D.6.3. Let $M/L/K$ be a tower of fields, with L/K finite and separable. Write $L \cong K[x]/\langle f(x) \rangle$ for $f(x) \in K[x]$ irreducible, and suppose that we have the factorisation $f(x) = g_1(x) \cdots g_r(x) \in M[x]$. Then

$$L \otimes_K M \cong \prod_{i=1}^r M[x]/\langle g_i(x) \rangle.$$

Finally, we connect the discrete absolute values on a number field with the factorisation of its defining polynomial in $\mathbb{Q}_p$. This provides an interesting example of using local (i.e., p -adic) tools to prove facts about global (i.e., number field) objects.

Theorem D.6.3. Let $L/\mathbb{Q}$ be a number field; say $L = \mathbb{Q}(\theta)$, where θ has minimal polynomial $f(x) \in \mathbb{Q}[x]$. Then the inequivalent extensions of the p -adic absolute value $|\cdot|_p$ to

L are in bijection with the irreducible factors of $f(x)$ in $\mathbb{Q}_p[x]$. In particular, there are finitely many such extensions.

Proof. Let $f(x) = g_1(x) \cdots g_r(x) \in \mathbb{Q}_p[x]$ be the factorisation of f into irreducibles, and let $\widehat{L}_i := \mathbb{Q}_p[x]/\langle g_i(x) \rangle$, which is a p -adic field of degree $\deg(g_i)$. In particular, $\widehat{L}_i$ is complete by Proposition D.6.1. By Theorem D.6.2, $|\cdot|_p$ on $\mathbb{Q}_p$ extends uniquely to $\widehat{L}_i$; call this unique extension $|\cdot|_i$.

By Lemmas D.6.2 and D.6.3, we have a composition of maps

$$\tau : L \hookrightarrow L \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{i=1}^r \widehat{L}_i \rightarrow \widehat{L}_i.$$

Thus, we can define $|\cdot|_L$ on L by pulling back $|\cdot|_i$. In other words, for $\alpha \in L$, let

$$|\alpha|_L := |\tau(\alpha)|_i.$$

Thus, for each i we obtain a discrete absolute value $|\cdot|_L$ on L extending $|\cdot|_p$.

Conversely, suppose $|\cdot|$ is a discrete absolute value on L extending $|\cdot|_p$. Let $\widehat{L}$ denote its completion, which comes with an embedding $\iota : L \hookrightarrow \widehat{L}$. Note that $\mathbb{Q}_p(\iota(\theta))$ is complete and contains $\iota(L)$ as a dense subset, so by uniqueness of completions, we have $\widehat{L} = \mathbb{Q}_p(\iota(\theta))$. If $g(x) \in \mathbb{Q}_p[x]$ is the minimal polynomial of $\iota(\theta)$, then $f(\iota(\theta)) = 0$, so $g(x) = g_i(x)$ for some i . This forces $\widehat{L} = \widehat{L}_i$, finishing the proof. $\square$