Algebraic Number Theory

Dr V. Dokchitser

Michaelmas 2007

LaTeXed by Sebastian Pancratz

These notes are based on a course of lectures given by Dr V. Dokchitser in Part III of the Mathematical Tripos at the University of Cambridge in the academic year 2007–2008.

These notes have not been checked by Dr V. Dokchitser and should not be regarded as official notes for the course. In particular, the responsibility for any errors is mine — please email Sebastian Pancratz (`sfp25`) with any comments or corrections.

Contents

1 Number Fields **1**

1.1 Units . . . 1

1.2 Factorisation . . . 2

1.3 Ideals . . . 3

1.4 Ideal Class Groups . . . 4

1.5 Primes and Modular Arithmetic . . . 4

1.6 Factorising Primes . . . 6

2 Decomposition of Primes **13**

2.1 Action of Galois . . . 13

2.2 Decomposition Group . . . 14

2.3 Counting Primes . . . 16

2.4 Induced Representations . . . 18

2.5 Induction and Restriction . . . 18

2.6 Counting More Primes . . . 19

3 L-Series **21**

3.1 Convergence Properties . . . 21

3.2 Dirichlet L-Functions . . . 23

3.3 Primes in Arithmetic Progression . . . 26

3.4 Dirichlet Characters . . . 28

3.5 Artin L-Functions . . . 28

3.6 Properties of Artin L-Functions . . . 31

3.7 Density Theorems . . . 33

3.8 Appendix (Local Fields) . . . 35

3.8.1 Residue fields and ramification . . . 35

3.8.2 Galois groups . . . 36

3.8.3 Applications . . . 36

Chapter 1

Number Fields

Definition. A *number field* K is a finite field extension of $\mathbb{Q}$. Its *degree* is $[K : Q]$, i.e., its dimension as a $\mathbb{Q}$-vector space.

Definition. An algebraic number α is an *algebraic integer* if it satisfies a monic polynomial with integer coefficients. Equivalently, its minimal polynomial over $\mathbb{Q}$ should have integer coefficients.

Definition. Let K be a number field. Its *ring of integers* $\mathcal{O}_K$ consists of the elements of K which are algebraic integers.

Proposition 1.1. (i) $\mathcal{O}_K$ is a Noetherian ring.
(ii) $\operatorname{rank}_{\mathbb{Z}} \mathcal{O}_K = [K : \mathbb{Q}]$, i.e., $\mathcal{O}_K$ is a finitely generated abelian group under addition, and isomorphic to $\mathbb{Z}^{\oplus[K:\mathbb{Q}]}$.
(iii) For every $\alpha \in K$ there exists $n \in N$ with $\alpha n \in \mathcal{O}_K$.
(iv) $\mathcal{O}_K$ is the maximal subring of K which is finitely generated as an abelian group.
(v) $\mathcal{O}_K$ is integrally closed, i.e., if $f(X) \in \mathcal{O}_K[X]$ is monic and $f(\alpha) = 0$ for some $\alpha \in K$ then $\alpha \in \mathcal{O}_K$.

Example.

Number field K	Ring of integers $\mathcal{O}_K$
$\mathbb{Q}$	$\mathbb{Z}$
$\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z} - \{0, 1\}$ squarefree	$\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \pmod 4$,
	$\mathbb{Z}[(1 + \sqrt{d})/2]$ if $d \equiv 1 \pmod 4$
$\mathbb{Q}(\zeta_n)$, ζ_n a primitive nth root of unity	$\mathbb{Z}[\zeta_n]$

Example. $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ since $\zeta_3 = (-1 + \sqrt{-3})/2$, $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$.

1.1 Units

Definition. A *unit* in a number field K is an element $\alpha \in \mathcal{O}_K$ such that $\alpha^{-1} \in \mathcal{O}_K$. The group of units in K is denoted by $\mathcal{O}_K^\times$.

Example. For $K = \mathbb{Q}$ we have $\mathcal{O}_K = \mathbb{Z}$ and $\mathcal{O}_K^\times = \{\pm 1\}$. For $K = \mathbb{Q}(\sqrt{-3})$ we have $\mathcal{O}_K = \mathbb{Z}[(1 + \sqrt{-3})/2]$ and $\mathcal{O}_K^\times = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$.

Theorem 1.2 (Dirichlet's Unit Theorem)**.** Let K be a number field. Then $\mathcal{O}_K^\times$ is a finitely generated abelian group. More precisely,

$$\mathcal{O}_K^\times = \Delta \times \mathbb{Z}^{r_1+r_2-1}$$

where Δ is the finite group of roots of unity in K, and r_1 and r_2 denote the number of real embeddings $K \hookrightarrow \mathbb{R}$ and complex conjugate embeddings $K \hookrightarrow \mathbb{C}$ with image not contained in $\mathbb{R}$, so $r_1 + 2r_2 = [K : \mathbb{Q}]$.

Corollary 1.3. The only number fields with finitely many units are $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{-D})$, $D > 0$.

1.2 Factorisation

Example. $\mathbb{Z}$ has unique factorisation. We do not have this luxury in $\mathcal{O}_K$ in general, e.g., let $K = \mathbb{Q}(\sqrt{-5})$ with $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ then

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

where $2, 3, 1 \pm \sqrt{-5}$ are irreducible and $2, 3$ are not equal to $1 \pm \sqrt{-5}$ up to units.

Theorem 1.4 (Unique Factorisation of Ideals)**.** Let K be a number field. Then every non-zero ideal of $\mathcal{O}_K$ admits a factorisation into prime ideals. This factorisation is unique up to order.

Example. In $K = \mathbb{Q}(\sqrt{-5})$,

$$\begin{aligned}(6) = (2)(3) &= (2, 1 + \sqrt{-5})^2(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) \\ &= (1 + \sqrt{-5})(1 - \sqrt{-5}) = (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5})(2, 1 + \sqrt{-5})(3, 1 - \sqrt{5})\end{aligned}$$

where $(2, 1 + \sqrt{-5}), (3, 1 + \sqrt{-5}), (3, 1 - \sqrt{-5})$ are prime ideals.

Definition. Let $A, B \subset \mathcal{O}_K$ be ideals. Then A *divides* B, $A \mid B$, if there exists $C \subset \mathcal{O}_K$ such that $A \cdot C = B$. Equivalently, if in the prime factorisations

$$A = P_1^{m_1} \cdots P_k^{m_k}, \qquad B = P_1^{n_1} \cdots P_k^{n_k}$$

we have $m_i \leq m_i$ for all $1 \leq i \leq k$.

Remark. (i) For $\alpha, \beta \in \mathcal{O}_K$, $(\alpha) = (\beta)$ if and only if $\alpha = \beta u$ for some $u \in \mathcal{O}_K^\times$.
(ii) For ideals $A, B \subset \mathcal{O}_K$, $A \mid B$ if and only if $A \supset B$.
(iii) To multiply ideals, just multiply their generators, e.g.,

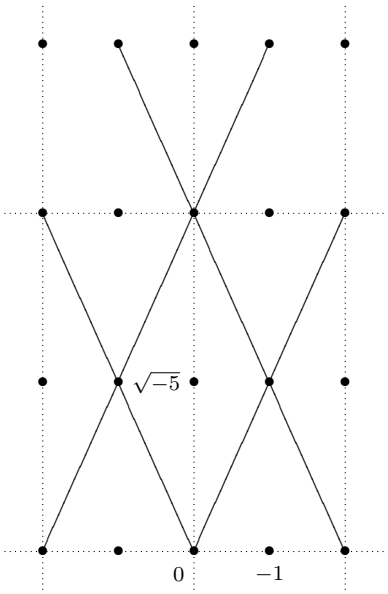
$$\begin{aligned}(2)(3) &= (6) \\ (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5}) &= (6, 2 + 2\sqrt{-5}, 3 + 3\sqrt{-5}, -4 + 2\sqrt{-5}) \\ &= (6, 1 + \sqrt{-5}) \\ &= (1 + \sqrt{-5}).\end{aligned}$$

(iv) Addition of ideals works completely differently, simply combine the generators, e.g.,

$$(2) + (3) = (2, 3) = (1) = \mathcal{O}_K.$$

1.3 Ideals

Example. $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.



An ideal is, in particular, a sublattice of $\mathcal{O}_K$. In fact, it always has finite index in $\mathcal{O}_K$.

Lemma 1.5. Let K be a number field, $\alpha \in \mathcal{O}_K - \{0\}$. Then there exists $\beta \in \mathcal{O}_K - \{0\}$ such that $\alpha\beta \in \mathbb{Z}$.

Proof. Let $f \in \mathbb{Z}[X]$ be the minimal polynomial of α, so

$$f(X) = (X - \alpha)(X - \gamma_1) \cdots (X - \gamma_n)$$

in a splitting field. Observe that $\alpha \prod \gamma_i = N \in \mathbb{Z} - \{0\}$, so

$$\prod \gamma_i = \frac{N}{\alpha} \in K$$

and all γ_i are algebraic integers, so

$$\beta = \prod \gamma_i \in \mathcal{O}_K - \{0\}$$

with $\alpha\beta = N \in \mathbb{Z} - \{0\}$. □

Corollary 1.6. Let $A \subset \mathcal{O}_K$ be a non-zero ideal. Then $[\mathcal{O}_K : A]$ is finite, i.e., $\operatorname{rank}_{\mathbb{Z}} A = [K : \mathbb{Q}]$.

Proof. Let $\alpha \in A - \{0\}$ and $\beta \in \mathcal{O}_K$ such that $\alpha\beta = N \in \mathbb{Z} - \{0\}$, and $N \in A \subset \mathcal{O}_K$ as A is an ideal.

$$\begin{aligned}[\mathcal{O}_K : A] &\leq [\mathcal{O}_K : (\alpha)] \leq [\mathcal{O}_K : (N)] \\ &= [\mathcal{O}_K : N\mathcal{O}_K] \\ &= |N|^{[K:\mathbb{Q}]} < \infty.\end{aligned}$$

□

Definition. The *norm* of a non-zero ideal A is the index $[\mathcal{O}_K : A]$.

Lemma 1.7. Let $\alpha \in \mathcal{O}_K - \{0\}$. Then

$$|N_{K/\mathbb{Q}}(\alpha)| = N\big((\alpha)\big).$$

Proof. Let $v_1, \ldots, v_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Write $T_\alpha \colon K \to K$ for the $\mathbb{Q}$-linear map $x \mapsto \alpha x$. Then

$$\begin{aligned} N_{K/\mathbb{Q}}(\alpha) &= \det T_\alpha \\ &= \det(\alpha v_1, \ldots, \alpha v_n) \\ &= \pm[\langle v_1, \ldots, v_n\rangle : \langle \alpha v_1, \ldots, \alpha v_n\rangle] \\ &= \pm[\mathcal{O}_K : \alpha\mathcal{O}_K] \\ &= \pm N((\alpha)). \end{aligned}$$

□

1.4 Ideal Class Groups

Let K be a number field. Define an equivalence relation $\sim$ on non-zero ideals by $A \sim B$ if $A = \lambda B$ for some $\lambda \in K^\times$. The *ideal class group* $\mathrm{Cl}(K)$ of K is the set of equivalence classes. This is in fact a group, the group structure comes from multiplication of ideals. The identity element is the class of principal ideals.

In particular, $\mathcal{O}_K$ is a unique factorisation domain if and only if $\mathrm{Cl}(K) = 1$.

Theorem 1.8. $\mathrm{Cl}(K)$ is finite.

Exercise. Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field. Then two non-zero ideals belong to the same class in $\mathrm{Cl}(K)$ if and only if the lattices they give in $\mathbb{C}$ are homeothetic, i.e., related by scaling and rotation about 0.

1.5 Primes and Modular Arithmetic

Definition. A *prime* P in a number field K is a non-zero prime ideal in $\mathcal{O}_K$. Its *residue field* is $\mathcal{O}_K/P$.

Example. $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$, $P = (p)$, $\mathcal{O}_K/P = \mathbb{Z}/(p) = \mathbb{F}_p$, where p is a prime number.

Definition. The *absolute residue degree* of P is

$$[\mathcal{O}_K/P : \mathbb{F}_p],$$

where $p = \operatorname{char} \mathcal{O}_K/P$.

Lemma 1.9. $\mathcal{O}_K/P$ is a finite field.

Proof. P is a prime ideal hence $\mathcal{O}_K/P$ is an integral domain and

$$|\mathcal{O}_K/P| = [\mathcal{O}_K : P] = N(P) < \infty,$$

hence $\mathcal{O}_K/P$ is a field. □

Note that $|\mathcal{O}_K/P| = N(P)$.

Example. $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$.

(i) $P = (2+i)$ then $\mathcal{O}_K/P \cong \mathbb{F}_5$ with representatives $0, i, i+1, 2i, 2i+1$.
(ii) $P = (3)$ then $\mathcal{O}_K/P \cong \mathbb{F}_9$.

Notation. If $A \subset \mathcal{O}_K$ is a non-zero ideal we say that

$$x \equiv y \pmod{A}$$

if $x - y \in A$.

Lemma 1.10. Let $A, B \subset \mathcal{O}_K$ be ideals with prime factorisations

$$A = \prod_{i=1}^{k} P_i^{m_i}, \qquad B = \prod_{i=1}^{k} P_i^{n_i}$$

where $m_i, n_i \geq 0$ and the P_i are distinct prime ideals. Then

(i) $A \cap B = \prod_i P_i^{\max\{m_i, n_i\}}$,
(ii) $A + B = \prod_i P_i^{\min\{m_i, n_i\}}$.

Proof. (i) This is the largest ideal contained in both A and B.
(ii) This is the smallest ideal containing both A and B. □

Lemma 1.11. Let P be prime in K. Then

(i) $|\mathcal{O}_K/P^n| = N(P)^n$,
(ii) $P^n/P^{n+1} \cong \mathcal{O}_K/P$ as $\mathcal{O}_K$-modules.

Proof. Note (ii) implies (i) by writing

$$|\mathcal{O}_K/P^n| = |\mathcal{O}_K/P||P/P^2| \cdots |P^{n-1}/P^n| = N(P)^n.$$

By unique factorisation, $P^n \neq P^{n+1}$. Pick $\pi \in P^n \setminus P^{n+1}$ and define

$$\phi\colon \mathcal{O}_K \to P^n/P^{n+1}, x \mapsto \pi x \bmod P^{n+1}$$

then

$$\begin{aligned} \ker\phi &= \{x : \pi x \in P^{n+1}\} \\ &= \{x : P^{n+1} \mid (\pi)(x)\} \\ &= \{x : P \mid (x)\} \\ &= P. \end{aligned}$$

Note $\operatorname{Im}\phi = P^n/P^{n+1}$ for otherwise $P^n \supsetneq \pi + P^n \supsetneq P^{n+1}$, a contradiction by unique factorisation. Now apply the First Isomorphism Theorem. □

Theorem 1.12 (Chinese Remainder Theorem)**.** Let K be a number field, $P_1, \ldots, P_k$ distinct prime ideals. Then

$$\mathcal{O}_K/P_1^{n_1} \cdots P_k^{n_k} \cong \mathcal{O}_K/P_1^{n_1} \times \cdots \times \mathcal{O}_K/P_k^{n_k}$$

via

$$x \bmod P_1^{n_1} \cdots P_k^{n_k} \mapsto (x \bmod P_1^{n_1}, \ldots, x \bmod P_k^{n_k}).$$

Proof. Let

$$\begin{aligned}\psi\colon \mathcal{O}_K &\to \mathcal{O}_K/P_1^{n_1} \times \cdots \times \mathcal{O}_K/P_k^{n_k}\\ x &\mapsto (x \bmod P_1^{n_1}, \ldots, x \bmod P_k^{n_k}).\end{aligned}$$

Then

$$\ker\psi = \{x : \forall i\ x \in P_i^{n_i}\} = \bigcap P_i^{n_i} = \prod P_i^{n_i}.$$

We claim $\operatorname{Im}\psi$ contains $(0,\ldots,0,1,0,\ldots,0)$, so ψ is surjective. Then by the First Isomorphism Theorem the result follows. Indeed, by Lemma 1.10,

$$P_j^{n_j} + P = \mathcal{O}_K = \mathcal{O}_K = (1)$$

where $P = \prod_{i\neq j} P_i^{n_i}$. Hence there exist $\alpha \in P_j^{n_j}$, $\beta \in P$ with $\alpha + \beta = 1$. Then $\beta \equiv 0 \pmod P$, $\beta \equiv 1 \pmod{P_j^{n_j}}$, so $\psi(\beta) = (0,\ldots,0,1,0,\ldots,0)$. □

Remark. The Chinese Remainder Theorem says we can solve congruences

$$\begin{aligned} x &\equiv a_1 \pmod{p_1^{n_1}}\\ &\vdots\\ x &\equiv a_k \pmod{p_k^{n_k}}\end{aligned}$$

for any given $a_1,\ldots,a_k$. This is called the Weak Approximation Theorem.

Corollary 1.13.

$$N(AB) = N(A)N(B).$$

Corollary 1.14.

$$N(A) \in A.$$

1.6 Factorising Primes

Example. Take primes in $\mathbb{Q}$ and factorise them in $\mathbb{Q}(i)$.

$$\begin{array}{lll}(2) = (1+i)^2 & (3) = (3) & (5) = (2+i)(2-i)\\ (7) = (7) & (11) = (11) & (13) = (3+2i)(3-2i)\end{array}$$

Remark. If P is a prime of $\mathbb{Q}(i)$ then $P \ni N(P) \in \mathbb{Z}$, so P contains a prime number p so $P \mid (p)$. In other words, factorising $2,3,5,7,\ldots$ we find all primes in $\mathbb{Q}(i)$.

Definition. Let L/K be an extension of number fields, and $A \subset \mathcal{O}_K$ an ideal. The *conorm* of A is the ideal $A\mathcal{O}_L$ of $\mathcal{O}_L$, i.e., it is generated by the elements of A. Equivalently, if $A = (\alpha_1,\ldots,\alpha_n)$ as an $\mathcal{O}_K$-ideal then $A\mathcal{O}_L = (\alpha_1,\ldots,\alpha_n)$ as an $\mathcal{O}_L$-ideal.

In particular, $(A\mathcal{O}_L)(B\mathcal{O}_L) = (AB)\mathcal{O}_L$, and if $M/L/K$ is a tower of number fields then $A\mathcal{O}_M = (A\mathcal{O}_L)\mathcal{O}_M$.

Definition. Let L/K be an extension of number fields. Say a prime Q of L *lies above* a prime P of K if $Q \mid P\mathcal{O}_L$. Equivalently, $Q \supset P$.

Lemma 1.15. Let L/K be an extension of number fields. Every prime Q of L lies above a unique prime of K: Q lies above $Q \cap \mathcal{O}_K$.

Proof. Let Q be a prime of L. Then $Q \cap \mathcal{O}_K$ is an ideal of $\mathcal{O}_K$, clearly also a prime ideal. $Q \cap \mathcal{O}_K \ni N(Q)$ hence is non-empty, so $Q \cap \mathcal{O}_K$ is a prime. So Q lies above $Q \cap \mathcal{O}_K$.

For uniqueness, note that if Q lies above P and P' then $Q \supset P + P' = (1)$ so $1 \in Q$, contradiction. □

Lemma 1.16. Suppose $Q \subset \mathcal{O}_L$ lies above $P \subset \mathcal{O}_K$. Then $\mathcal{O}_L/Q$ is an extension of $\mathcal{O}_K/P$.

Proof. Let $\phi\colon \mathcal{O}_K/P \to \mathcal{O}_L/Q, x \bmod P \mapsto x \bmod Q$. This is well-defined since $Q \supset P$, and this is a ring homomorphism sending 1 to 1, so it is an embedding of fields. □

Definition. If Q lies above P, its *relative residue degree* is

$$f_{Q/P} = [\mathcal{O}_L/Q : \mathcal{O}_K/P].$$

Its *ramification degree* $e_{Q/P}$ defined by

$$Q^{e_{Q/P}} \mid P\mathcal{O}_L, \qquad Q^{e_{Q/P}+1} \nmid P\mathcal{O}_L.$$

Therefore,

$$P\mathcal{O}_L = \prod_i Q_i^{e_{Q_i/P}}$$

and Q_i has residue field an extension of the residue field of P of degree $f_{Q_i/P}$.

Definition.
- If $f_{Q/P} \neq 1$ then Q/P is *inert*.
- If $e_{Q/P} \neq 1$ then Q/P is *ramified*.
- If $e_{Q/P} = 1$ then Q/P is *unramified*.

Lemma 1.17. Suppose $M/L/K$ is a tower of number fields and we have primes R over Q over P in M, L, K, respectively. Then

(i) $e_{R/P} = e_{R/Q}e_{Q/P}$,
(ii) $f_{R/P} = f_{R/Q}f_{Q/P}$.

Proof. (i) Just factorise $P\mathcal{O}_M$.
(ii) By the tower law,

$$[\mathcal{O}_M/R : \mathcal{O}_K/P] = [\mathcal{O}_M/R : \mathcal{O}_L/Q][\mathcal{O}_L/Q : \mathcal{O}_K/P].$$ □

Proposition 1.18. Let L/K be an extension of number fields, $A \subset \mathcal{O}_K$ a non-zero ideal. Then

$$N(A\mathcal{O}_L) = N(A)^{[L:K]}.$$

Proof. If $\alpha \in K$ then

$$|N_{K/\mathbb{Q}}(\alpha)|^{[L:K]} = |N_{L/\mathbb{Q}}(\alpha)|.$$

As $|N_{K/\mathbb{Q}}(\alpha)| = N\big((\alpha)\big)$ and similarly over L, we have

$$N(A\mathcal{O}_L) = N(A)^{[L:K]}$$

if A is principal. In general, $A^k = A \cdots A$ is principal for some $k \in \mathbb{N}$ by finiteness of $\mathrm{Cl}(K)$. As $N(A)^k = N(A^k)$, the result follows. □

Theorem 1.19. Let L/K be an extension of number fields. Let P be a prime of K and decompose

$$P\mathcal{O}_L = \prod_{i=1}^{m} Q_i^{e_i}$$

with $e_i = e_{Q_i/P}$ for distinct primes Q_i. Then

$$\sum_{i=1}^{m} e_i f_i = [L : K].$$

Theorem 1.20 (Kummer–Dedekind)**.** Let L/K be an extension of number fields, suppose $\mathcal{O}_L \supset \mathcal{O}_K[\alpha]$ with finite index N. Let the minimal polynomial of α be $f(X) \in \mathcal{O}_K[X]$.

Let P be a prime of K with $\gcd(N, |\mathcal{O}_K/P|) = 1$. If $f(X) \equiv \prod_{i=1}^{m} \bar{g}_i^{e_i} \pmod{P}$ for distinct irreducibles $\bar{g}_i$ and $\bar{g}_i \equiv g_i \pmod{P}$ then

$$P\mathcal{O}_L = \prod_{i=1}^{m} Q_i^{e_i}$$

with distinct primes Q_i and

$$\begin{aligned} e_{Q_i/P} &= e_i, \\ f_{Q_i/P} &= \deg \bar{g}_i(X), \\ Q_i &= P\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L. \end{aligned}$$

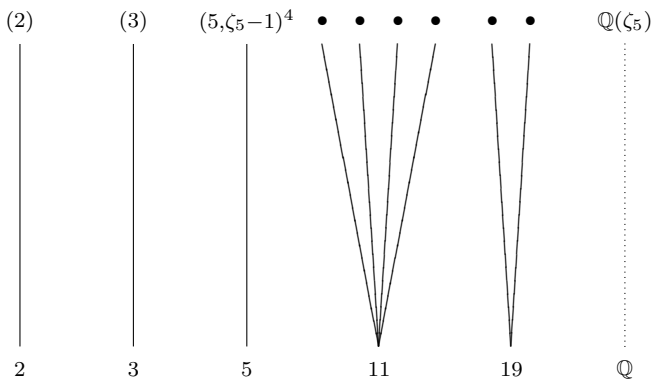
Remark. We cannot always assume α is such that $[\mathcal{O}_L : \mathcal{O}_K[\alpha]] = 1$. But by the Primitive Element Theorem, we can find α such that $[\mathcal{O}_L : \mathcal{O}_K[\alpha]] < \infty$.

Example. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_5)$, $\mathcal{O}_L = \mathbb{Z}[\zeta_5]$ and $\alpha = \zeta_5$. Then $N = 1$ and

$$f(X) = \frac{X^5 - 1}{X - 1} = X^4 + X^3 + X^2 + X + 1.$$

For the prime integers $2, \ldots, 19$ we have the following.

(2) $f(X) \pmod 2$ is irreducible
(3) $f(X) \pmod 3$ is irreducible
(5) $f(X) \equiv (X-1)^4 \pmod 5$
(7) $f(X) \pmod 7$ is irreducible
(11) $f(X) \equiv (X-4)(X-9)(X-5)(X-3) \pmod{11}$
(13) $f(X) \pmod{13}$ is irreducible
(17) $f(X) \pmod{17}$ is irreducible
(19) $f(X) \equiv (X^2+5X+1)(X^2-4X+1) \pmod{19}$



Definition. Let L/K be an extension of number fields, P prime in K, $P\mathcal{O}_L = \prod_{i=1}^{N} Q_i^{e_i}$ for distinct primes Q_i in L. Then P

- *splits completely* if $N = [L : K]$
- *splits* if $N > 1$
- is *totally ramified* if $N = 1 = f_{Q/P}$, $e_{Q/P} = [L : K]$.

If L/K is Galois then it turns out that for all i, j

$$e_{Q_i/P} = e_{Q_j/P}, \qquad f_{Q_i/P} = f_{Q_j/P}.$$

In this case say P is

- *ramified* if $e_{Q_i/P} > 1$,
- *unramified* if $e_{Q_i/P} = 1$,
- *inert* if $P\mathcal{O}_L$ is prime.

Example. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_{p^n})$ for an odd prime p. Then $\mathcal{O}_L = \mathbb{Z}[\zeta_{p^n}]$. In Kummer–Dedekind, take $\alpha = \zeta$ so

$$f(X) = \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1} \equiv (X - 1)^{p^n - p^{n-1}} \pmod{p}.$$

So p is totally ramified in $\mathbb{Q}(\zeta_{p^n})$. If $q \neq p$ is prime then $X^{p^n} - 1$ has distinct roots in $\bar{\mathbb{F}}_q$ as $\gcd(X^{p^n} - 1, p^n X^{p^n - 1}) = 1$ in $\mathbb{F}_q[X]$, hence $f(X)$ has distinct roots in $\bar{\mathbb{F}}_q$, so q is unramified in $\mathbb{Q}(\zeta_{p^n})$.

Proof (Theorem 1.20). Write $A = \mathcal{O}_K[\alpha]$, $\mathbb{F} = \mathcal{O}_K/P$, $\operatorname{char} \mathcal{O}_K/P = p$. Considering the map $\alpha \mapsto X$, we see that

$$\begin{aligned} A/(P, g_i(\alpha)) &\cong \mathcal{O}_K[X]/(f(X), P, g_i(X)) \\ &\cong \mathbb{F}[X]/(\bar{f}(X), \bar{g}_i(X)) \\ &= \mathbb{F}[X]/(\bar{g}_i(X)) \end{aligned}$$

is a field of degree $\deg g_i(X)$ over $\mathbb{F}$ as $g_i(X)$ is irreducible.

Consider $\phi\colon \mathcal{O}_L \xrightarrow{\cdot N} \mathcal{O}_K[\alpha] = A \to A/(P, g_i(\alpha))$. ϕ is surjective, as $\cdot N$ is an isomorphism on $A/(P, g_i(\alpha))$. If $x \in \ker \phi$ then $Nx \in PA + g_i(\alpha)A$ but $px \in PA \subset PA + g_i(\alpha)A$ so $x \in PA + g_i(\alpha)A$ as $\gcd(N, p) = 1$. In particular, $x \in Q_i$. Conversely, if $x \in Q_i$ then $Nx \in PN\mathcal{O}_L + g_i(\alpha)N\mathcal{O}_L \subset PA + g_i(\alpha)A$ so $x \in \ker \phi$. Thus

$$\mathcal{O}_L/Q_i \cong A/(P, g_i(\alpha))$$

so Q_i is prime and $f_{Q_i/P} = \deg \bar{g}_i$.

For $i \neq j$, $\gcd(\bar{g}_i(X), \bar{g}_j(X)) = 1$ so we find $\lambda(X), \mu(X) \in \mathcal{O}_K[X]$ such that $\lambda(X)g_i(X) + \mu(X)g_j(X) \equiv 1 \pmod{P}$. Then

$$Q_i + Q_j = P\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L + g_j(\alpha)\mathcal{O}_L \ni \lambda(\alpha)g_i(\alpha) + \mu(\alpha)g_j(\alpha)$$

so $1 \in Q_i + Q_j$ and $Q_i \neq Q_j$.

Note that

$$\prod_i Q_i^{e_i} = \prod_i (P\mathcal{O}_l + g_i(\alpha)\mathcal{O}_L)^{e_i}$$

$$\begin{aligned} &\subset P\mathcal{O}_L + \Big(\prod_i g_i(\alpha)^{e_i}\Big)\mathcal{O}_L \\ &\subset P\mathcal{O}_L \end{aligned}$$

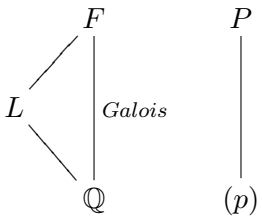
as $\prod_i g_i(\alpha)^{e_i} \equiv f(\alpha) \equiv 0 \pmod{P}$. But

$$N\Big(\prod_i Q_i^{e_i}\Big) = \prod_i \big(|\mathbb{F}|^{f_i}\big)^{e_i} = |F|^{\deg f} = N(P\mathcal{O}_L)$$

by Proposition 1.18. Hence $P\mathcal{O}_L = \prod_i Q_i^{e_i}$. □

Proposition 1.21. Suppose $L/\mathbb{Q}$ is finite, $\alpha \in \mathcal{O}_L$ such that $L = \mathbb{Q}(\alpha)$ and the minimal polynomial of α is $f(X) \in \mathbb{Z}[X]$. Suppose $f(X) \bmod p$ has distinct roots in $\bar{F}_p$. Then $[\mathcal{O}_L : \mathbb{Z}[\alpha]]$ is coprime to p. (So Theorem 1.20 applies.)

Proof. Let F be a splitting field of f, $f(X) = \prod_{i=1}^n (X - \alpha_i)$. Pick a prime P in F above p.



Then modulo P, $\bar{f}(X) = \prod_{i=1}^n (X - \bar{\alpha}_i)$, where $\bar{\alpha}_i$ are distinct as $\mathcal{O}_F/P$ is a finite extension of $\mathbb{F}_p$, so

$$\prod_{i<j} (\alpha_i - \alpha_j) \not\equiv 0 \pmod{P}.$$

Let $\beta_1, \ldots, \beta_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_L$, so

$$\begin{pmatrix} 1 \\ \alpha_1^2 \\ \vdots \\ \alpha_1^{n-1} \end{pmatrix} = M \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}$$

where $M \in GL_n(\mathbb{Z})$ with $\det M = [\mathcal{O}_L : \mathbb{Z}[\alpha]]$. Write $\sigma_1, \ldots, \sigma_n \colon L \hookrightarrow F$ for the embeddings with $\sigma_i(\alpha_1) = \alpha_i$. Then

$$\begin{aligned} \prod_{i<j} (\alpha_i - \alpha_j) &= \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1} \end{vmatrix} \\ &= (\det M) \begin{vmatrix} \beta_1 & \sigma_2(\beta_1) & \ldots & \sigma_n(\beta_1) \\ \beta_2 & \sigma_2(\beta_2) & \ldots & \sigma_n(\beta_2) \\ \vdots & \vdots & & \vdots \\ \beta_n & \sigma_2(\beta_n) & \ldots & \sigma_n(\beta_n) \end{vmatrix} \\ &= [\mathcal{O}_L : \mathbb{Z}[\alpha]] B \end{aligned}$$

for some $B \in \mathcal{O}_F$.

Hence $p \nmid [\mathcal{O}_L : \mathbb{Z}[\alpha]]$. □

Proposition 1.22. Let K be a number field, P a prime of K. Suppose $f(X) \in \mathcal{O}_K[X]$ is with respect to P, i.e.,

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

with $P \mid (a_i)$ for $i = 0, \ldots, n-1$ and $P^2 \nmid (a_0)$. Then $f(X)$ is irreducible, and if α is a root then $K(\alpha)/K$ is totally ramified.

Proof. See *Local Fields*. □

Chapter 2

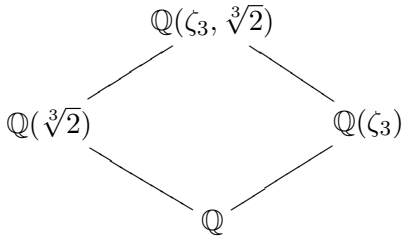
Decomposition of Primes

2.1 Action of Galois

Let F/K be a Galois extension of number fields. Recall that $\mathrm{Gal}(F/K) = \mathrm{Aut}_K(F)$.

- F/K is normal, i.e., if $f(X) \in K[X]$ is irreducible and it has a root in F then all its roots lie in F.
- $|\mathrm{Gal}(F/K)| = [F : K]$.
- $\{H \leq \mathrm{Gal}(F/K)\}$ is in bijection with $\{L : K \subset L \subset F\}$ via $H \mapsto F^H$ and $L \mapsto \mathrm{Gal}(F/L)$.

Example.



Lemma 2.1. Suppose F/K is Galois, $g \in \mathrm{Gal}(F/K)$. Then

(i) $\alpha \in \mathcal{O}_F \implies g(\alpha) \in \mathcal{O}_F$; so $\mathrm{Gal}(F/K)$ acts on $\mathcal{O}_F$.
(ii) If $A \subset \mathcal{O}_F$ is an ideal then $g(A)$ is an ideal in $\mathcal{O}_F$.
(iii) If $A, B \subset \mathcal{O}_F$ are ideals then $g(AB) = g(A)g(B)$ and $g(A + B) = g(A) + g(B)$.
(iv) Suppose Q is a prime of F above P of K. Then $g(Q)$ is a prime of F above P, so $\mathrm{Gal}(F/K)$ acts on the primes of F above P.
(v) $e_{Q/P} = e_{g(Q)/P}$, $f_{Q/P} = f_{g(Q)/P}$.

Proof. Clear. □

Example. Let $K = \mathbb{Q}$, $F = \mathbb{Q}(i)$, so $\mathcal{O}_F = \mathbb{Z}[i]$, $\mathrm{Gal}(F/K) = \{\iota, c = \bar{\cdot}\}$. Note c fixes $(1 + i)$, c fixes the lattice of (3), and $(5) = (2 + i)(2 - i)$ and c swaps the two factors.

Theorem 2.2. Let F/K be a Galois extension of number fields, P a prime of K. Then $\mathrm{Gal}(F/K)$ *acts transitively* on the primes of F above P.

Proof. Let $Q_1, \ldots, Q_n$ be the primes of F above P. We are required to prove that there exists $g \in \mathrm{Gal}(F/K)$ such that $g(Q_1) = Q_2$. Pick $x \in \mathcal{O}_F$ with $x \equiv 0 \pmod{Q_1}$,

i.e., $x \in Q_1$, and $x \not\equiv 0 \pmod{Q_i}$ for $1 < i$, i.e., $x \notin Q_i$. This exists by the Chinese Remainder Theorem. Then

$$\prod_{h \in \mathrm{Gal}(F/K)} h(x) \in \mathcal{O}_K \cap Q_1 = P \subset Q_2.$$

So for some $g \in \mathrm{Gal}(F/K)$, $g(x) \equiv 0 \pmod{Q_2}$, as Q_2 is a prime ideal, but $g(x) \equiv 0 \pmod{g(Q_1)}$ and this is the only such prime above P. □

Corollary 2.3. Suppose F/K is Galois. If Q_1, Q_2 are primes of F above P a prime of K then

$$e_{Q_1/P} = e_{Q_2/P}, \qquad f_{Q_1/P} = f_{Q_2/P}.$$

2.2 Decomposition Group

Suppose F/K is a Galois extension of number fields, P a prime of K, and $Q = Q_1, \ldots, Q_n$ the primes above P.

Definition. The *decomposition group* D_Q of Q above P is the subgroup of $\mathrm{Gal}(F/K)$ fixing Q, i.e.,

$$D_Q = \mathrm{Stab}_{\mathrm{Gal}(F/K)}(Q).$$

Remark. $g \in D_Q$ fixes Q, so it acts on $\mathcal{O}_F/Q$ by $x + Q \mapsto g(x) + Q$, and given an automorphism of $\mathcal{O}_F/Q$ fixing $\mathcal{O}_K/P$ there is a natural map

$$D_Q \to \mathrm{Gal}\big((\mathcal{O}_F/Q)/(\mathcal{O}_K/P)\big).$$

Example. Let $K = \mathbb{Q}$, $F = \mathbb{Q}(i)$, so $\mathcal{O}_F = \mathbb{Z}[i]$, $\mathrm{Gal}(F/K) = \{\iota, c = \bar{\cdot}\}$. Look at (3), its residue field is $\mathbb{F}_9$. $c \in D_{(3)}$, $c(a + bi) = a - bi = (a + bi)^3 \pmod{(3)}$, i.e., c acts as $x \mapsto x^3$ on $\mathbb{F}_9$, i.e., as the Frobenius automorphism.

Theorem 2.4. The map $D_Q \to \mathrm{Gal}\big((\mathcal{O}_F/Q)/(\mathcal{O}_K/P)\big)$ is surjective.

Proof. Pick $\beta \in \mathcal{O}_F/Q$ with $\mathcal{O}_F/Q = \mathcal{O}_K/P[\beta]$, e.g., β a generator for $(\mathcal{O}_F/Q)^\times$. Say β has minimal polynomial $f(X)$ over $\mathcal{O}_K/P$ with roots $\beta = \beta_1, \beta_2, \ldots, \beta_n$. Note $\beta_i \in \mathcal{O}_F/Q$ since F/K is Galois.

It suffices to show that there exists $g \in \mathrm{Gal}(F/K)$ such that $g(Q) = Q$ and $g(\beta) = \beta_2$.

Pick $\alpha \in \mathcal{O}_F$ with $\alpha \equiv \beta \pmod{Q}$ and $\alpha \equiv 0 \pmod{Q'}$ for all $Q' \neq Q$ above P. Say $\mathcal{F}(X)$ is the minimal polynomial of α over K with roots $\alpha = \alpha_1, \ldots, \alpha_r$. Note $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_F$.

$\mathcal{F}(X) \bmod Q$ has β as a root, its roots are $\alpha_i \bmod Q$, so is divisible by the minimal polynomial of β, hence has β_2 as a root. Without loss of generality, $\alpha_2 \equiv \beta_2 \pmod{Q}$.

Pick $g \in \mathrm{Gal}(F/K)$ with $g(\alpha) = \alpha_2$. Then $g(\alpha) \not\equiv 0 \pmod{Q}$ so $g(Q) = Q$ so $g \in D_{Q/P}$. Also $g(\beta) = \beta_2$ as $\beta \equiv \alpha \pmod{Q}$, $\beta_2 \equiv g(\alpha) \pmod{Q}$. □

Corollary 2.5. Let K be a number field, $f(X)$ monic irreducible over K of degree n and with coefficients in $\mathcal{O}_K$. Suppose F is the splitting field of $f(X)$. Let P be a prime of K and assume

$$f(X) = g_1(X) \cdots g_m(X) \pmod{P}$$

with $g_i(X)$ distinct irreducible polynomials over $\mathcal{O}_K/P$. Then $\mathrm{Gal}(F/K) \subset S_n$ contains an element of cycle type $(\deg g_1, \ldots, \deg g_m)$.

Proof. Let Q be a prime of F above P. Let $\alpha_1, \dots, \alpha_n$ be the roots of $f(X)$, note that $\alpha_i \bmod Q$ are roots of $f(X) \bmod P$, and are distinct in $\mathcal{O}_F/Q$.

Therefore, the action of $g \in D_{Q/P}$ on $\alpha_1, \dots, \alpha_n$ is exactly the same as on $\alpha_1 \bmod Q, \dots, \alpha_1 \bmod Q$.

Take $g \in D_{Q/P}$ which maps to the generator of $\mathrm{Gal}\big((\mathcal{O}_F/Q)/(\mathcal{O}_K/P)\big)$, it has the correct cycle type in its action on $\alpha_i \bmod Q$. □

Definition. Suppose F/K is a Galois extension of number fields, Q a prime above P. The *inertia group* $I_{Q/P}$ is the subgroup of $D_{Q/P}$ that acts trivially on $\mathcal{O}_F/Q$.

$$I_{Q/P} = \ker\big(D_{Q/P} \to (\mathcal{O}_F/Q)/(\mathcal{O}_K/P)\big).$$

This is surjective, so

$$D_{Q/P}/I_{Q/P} \cong \mathrm{Gal}\big((\mathcal{O}_F/Q)/(\mathcal{O}_K/P)\big).$$

The right-hand side is cyclic generated by the Frobenius element $\phi\colon x \mapsto x^{|\mathcal{O}_K/P|}$. The *(arithmetic) Frobenius element* $\mathrm{Frob}_{Q/P}$ is the element of $D_{Q/P}/I_{Q/P}$ that ϕ corresponds to, e.g., in the corollary, $I_{Q/P}$ is trivial and $\mathrm{Frob}_{Q/P}$ acts as an element in S_n of cycle type $(\deg g_1, \dots, \deg g_m)$.

Lemma 2.6. Suppose F/K is Galois, Q a prime of F above P, a prime of K. Then

(i) $|D_{Q/P}| = e_{Q/P} f_{Q/P}$,
(ii) the order of $\mathrm{Frob}_{Q/P}$ is $f_{Q/P}$,
(iii) $|I_{Q/P}| = e_{Q/P}$.

If $K \subset L \subset F$ is an intermediate field and S a prime below Q then

(iv) $D_{Q/S} = D_{Q/P} \cap \mathrm{Gal}(F/L)$,
(v) $I_{Q/S} = I_{Q/P} \cap \mathrm{Gal}(F/L)$.

Proof. (i) If n is the number of primes of F above P then

$$n|D_{Q/P}| = |\mathrm{Gal}(F/K)|$$

using Orbit-Stabiliser and Theorem 2.2

$$\begin{aligned} &= [F : K] \\ &= \sum_{i=1}^{n} e_i f_i \\ &= n e_{Q/P} f_{Q/P}. \end{aligned}$$

(ii)

$$\begin{aligned} f_{Q/P} &= [\mathcal{O}_F/Q : \mathcal{O}_K/P] \\ &= \big|\mathrm{Gal}\big((\mathcal{O}_F/Q)/(\mathcal{O}_K/P)\big)\big| \end{aligned}$$

which is the order of the Frobenius element.
(iii) $|D_{Q/P}| = |I_{Q/P}|$(order of Frobenius).
(iv) From the definition.

(v) From the definition. □

Example. Let $K = \mathbb{Q}$, $F = \mathbb{Q}(\zeta_p)$, so $\mathcal{O}_F = \mathbb{Z}[\zeta_p]$. Let $q \neq p$ be a prime number and Q a prime of F above (q).

Then F/K is unramified at Q, so $I_{Q/(q)} = \{\iota\}$. $\mathrm{Frob}_{Q/(q)}$ acts on $\mathcal{O}_F/Q$ by $x \mapsto x^q$. Note $\mathcal{O}_K/(q)$ is generated by the image of ζ_p, so $\mathrm{Frob}^n_{Q/(q)} = \iota$ if and only if $\mathrm{Frob}^n_{Q/(q)}(\zeta_p) = \zeta_p$ mod Q if and only if $\zeta_p^{q^n} = \zeta_p \mod Q$ if and only if $\zeta_p^{q^n} = \zeta_p$, because ζ_p^i are distinct modulo Q for $0 < i < p$ as $X^p - 1$ has distinct roots modulo Q. That is, the order of $\mathrm{Frob}_{Q/(q)}$ is the order of q in $(\mathbb{Z}/p\mathbb{Z})^\times$, which is thus also equal to $f_{Q/(q)}$.

2.3 Counting Primes

Lemma 2.7. Let F/K be a Galois extension of number fields.

(i) Primes of K are in bijection with $\mathrm{Gal}(F/K)$-orbits of primes of F, via $P \mapsto \{\text{primes of } F \text{ above } P\}$.
(ii) If Q is a prime of F above P then $gD_{Q/P} \mapsto g(Q)$ for $g \in \mathrm{Gal}(F/K)$ is a $\mathrm{Gal}(F/K)$-set isomorphism from $G/D_{Q/P}$ to the set of primes of F over P.
(iii) $D_{g(Q)/P} = gD_{Q/P}g^{-1}$, $I_{g(Q)/P} = gI_{Q/P}g^{-1}$ for $g \in \mathrm{Gal}(F/K)$.

Proof. (i) Follows from the transitivity of $\mathrm{Gal}(F/K)$ on primes above P, see Theorem 2.2.
(ii) Elementary group theory check.
(iii) Elementary check. □

Remark. Suppose G is a finite group. Then

$$\begin{array}{ccc} \{\text{transitive } G\text{-sets}\}/\cong & \xleftrightarrow{1-1} & \{\text{subgroups } D \leq G\}/\text{conjugacy} \\ X & \longmapsto & \mathrm{Stab}(\text{point}) \\ G/D & \longmapsto & D \end{array}$$

In particular, $X \cong G/\mathrm{Stab}(\text{point})$.

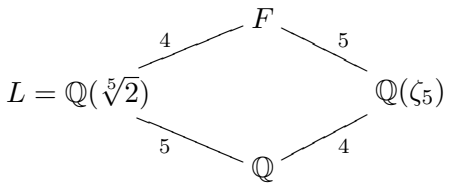
Corollary 2.8. Let F/K be a Galois extension of number fields, L an intermediate field. Let P be a prime of K, $Q = Q_1, \ldots, Q_n$ the primes of F above P. Then

$$\begin{array}{ccc} \{\text{primes of } L \text{ above } P\} & \longleftrightarrow & \{\mathrm{Gal}(F/L)\text{-orbits of } Q_1, \ldots, Q_n\} \\ & \longleftrightarrow & \{\mathrm{Gal}(F/L) - D_Q \text{ double cosets in } \mathrm{Gal}(F/K)\} \end{array}$$

via the map taking S to the elements of G that take Q to a prime above S.

Remark (Double cosets)**.** Suppose $D, H \leq G$ then a $D - H$ double coset is a set of the form $DgH = \{dgh : d \in D, h \in H\}$.

Example. Let $K = \mathbb{Q}$, $F = \mathbb{Q}(\zeta_5, \sqrt[5]{2})$, a splitting field of $X^5 - 2$.



Let $p = 73$. Note p is unramified in $\mathbb{Q}(\zeta_5)$, and p is unramified in $\mathbb{Q}(\sqrt[5]{2})$, as $X^2 - 5$ has distinct roots modulo 73. Thus, if Q is a prime of F above 73 then $e_Q \mid 4$, $e_Q \mid 5$, hence $e_Q = 1$ and $I_Q = 1$.

73 generates $(\mathbb{Z}/5\mathbb{Z})^\times$, so there exist a unique prime in $\mathbb{Q}(\zeta_5)$ above it, with residue degree 4.

D_Q/I_Q is cyclic, hence D_Q is cyclic of order divisible by 4. Thus $D_Q = C_4 \leq S_5$.

Without loss of generality, D_Q fixes $\sqrt[5]{2}$.

So the set of primes of F above 73 is isomorphic to $\mathrm{Gal}(F/K)/D_Q$ as a $\mathrm{Gal}(F/K)$-set, and also

$$\mathrm{Gal}(F/K)/D_Q \cong \{\sqrt[5]{2}, \zeta_5\sqrt[5]{2}, \zeta_5^2\sqrt[5]{2}, \zeta_5^3\sqrt[5]{2}, \zeta_5^4\sqrt[5]{2}\}.$$

Therefore, there exist two primes above 73 in $\mathbb{Q}(\sqrt[5]{2})$.

Note if $D, H \leq G$ are finite groups then $H - D$ double cosets are H-orbits on G/D (G acts on the left, HgD), which are the same as D-orbits on $H\backslash G$ (G acts on $H\backslash G$ via $x(Hg) = Hgx^{-1}$).

Lemma 2.9. Suppose F/K is a Galois extension of number fields, and L is an intermediate field. Let $G = \mathrm{Gal}(F/K)$, $H = \mathrm{Gal}(F/L)$, $D = D_Q$ the decomposition group of a prime Q of F above a prime P of K. Then

$$\begin{aligned} \{\text{embeddings } L \hookrightarrow F\} &\to H\backslash G \\ g \circ \iota &\mapsto Hg^{-1} \end{aligned}$$

is a G-set isomorphism. In particular, the number of primes of L above P is equal to the number of D_Q-orbits on the set of embeddings $L \hookrightarrow F$.

Proof. Elementary check. □

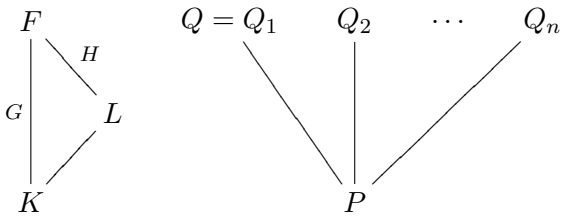
Remark. (i) If G is a finite group, X a G-set, then

$$\#\ G\text{-orbits on } X = \langle \mathbb{I}, \mathbb{C}[X] \rangle.$$

(ii) If X is a transitive G-set, S the stabiliser of a point in X, then

$$\mathbb{C}[X] = \mathrm{Ind}_S^G \mathbb{I}.$$

(iii) Suppose



Then the number of H-orbits on primes above P is equal to

$$\langle \mathbb{I}_H, \mathbb{C}\{\text{primes above } P\}\rangle_H = \langle \mathbb{I}_H, \operatorname{Res}^G_H \operatorname{Ind}^G_D \mathbb{I}\rangle_H.$$

If $D = D_Q$ then the number of D-orbits on embeddings $L \hookrightarrow F$ is equal to

$$\langle \mathbb{I}_D, \{L \hookrightarrow F\}\rangle_D = \langle \mathbb{I}_D, \operatorname{Res}^G_D \operatorname{Ind}^G_H \mathbb{I}\rangle_D.$$

That these are equal is an instance of Frobenius reprocity (see *Representation Theory*).

2.4 Induced Representations

Let G be a finite group. The *permutation representation* is the following. If G acts on $X = \{x_1, \ldots, x_n\}$ we associate to it the representation of $\mathbb{C}[X]$ of dimension $n = |X|$ with basis $x_1, \ldots, x_n$ and action

$$g \sum \lambda_i x_i = \sum \lambda_i g(x_i).$$

The number of G-orbits on X is

$$\langle \mathbb{I}, \mathbb{C}[X]\rangle.$$

The character formula is

$$\chi_{\mathbb{C}[X]}(g) = \#\text{ of fixed points of } g \text{ on } X.$$

Let $H \leq G$ of index n, V an H-represention. Officially,

$$\operatorname{Ind}^G_H V = \operatorname{Hom}_{\mathbb{C}[H]}(\mathbb{C}[G], V)$$

so $\dim \operatorname{Ind}^G_H V = n \dim V$. Concretely, if $g_1, \ldots, g_n$ are coset representatives for H take $\operatorname{Ind}^G_H V = V \oplus \cdots \oplus V$ (n times) with G-action

$$g(0, \ldots, 0, v, 0, \ldots, 0) = (0, \ldots, 0, h(v), 0, \ldots, 0)$$

where v is in the ith place, $h(v)$ in the jth place and $gg_i = g_j h$ for some $h \in H$.

Note if $V = \mathbb{I}$ then $\operatorname{Ind}^G_H V = \mathbb{C}[G/H]$.

We have the character formula

$$\chi_{\operatorname{Ind}^G_H V}(g) = \frac{1}{|H|} \sum_{\substack{z \in G \\ zgz^{-1} \in H}} \chi_V\left(zgz^{-1}\right).$$

2.5 Induction and Restriction

Consider the character tables of S_3 and S_4.

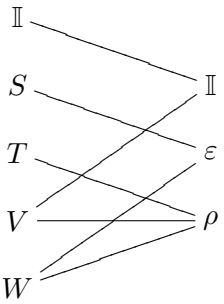
	S_3	1	(xy)	(xyz)
	$\mathbb{I}$	1	1	1
sign	ε	1	-1	1
acs on Δ	ρ	2	0	-1

	S_4	1	(xy)	(xyz)	$(xy)(zw)$	$(xyzw)$
	$\mathbb{I}$	1	1	1	1	1
	S	1	-1	1	1	-1
$S_4/\text{Kleingroup} \cong S_3$	T	2	0	-1	2	0
$\mathbb{C}[\{1,2,3,4\}] - \mathbb{I}$	V	3	1	0	-1	-1
$V \otimes S$	W	3	-1	0	-1	1

We observe the following identities

$$\begin{aligned} \operatorname{Res}\mathbb{I} &= \mathbb{I} & \operatorname{Res} S &= \varepsilon & \operatorname{Res} T &= \rho \\ \operatorname{Res} V &= \rho \oplus \mathbb{I} & \operatorname{Res} W &= \rho \oplus \varepsilon & & \\ \operatorname{Ind}\mathbb{I} &= \mathbb{I} \oplus V & \operatorname{Ind}\varepsilon &= S \oplus W & \operatorname{Ind}\rho &= T \oplus V \oplus W \end{aligned}$$

which we can visualise as follows:



Theorem 2.10 (Frobenius reciprocity)**.** $H \leq G$, V an H-representation, W a G-representation. Then

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

Proof. TODO. Provide reference. □

Theorem 2.11 (Mackey's formula)**.** $D, H \leq G$, ρ a D-representation. Let $X = \{x_1, \ldots, x_n\}$ be a set of $H - D$ double coset representatives. For $x \in X$ let $\rho^x(xgx^{-1}) = \rho(g)$, a representation of xDx^{-1}. Then

$$\operatorname{Res}^G_H \operatorname{Ind}^G_D \rho = \bigoplus_{x \in X} \operatorname{Ind}^H_{xDx^{-1}\cap H} \operatorname{Res}^{xDx^{-1}}_{xDx^{-1}\cap H} \rho^x.$$

Proof. TODO. Provide reference. □

2.6 Counting More Primes

Fix the following setting. Let F/K be a Galois extension of number fields, $G = \operatorname{Gal}(F/K)$, $H \leq G$, $L = F^H$, Q a prime of F above S a prime of L above P a prime of K, $\mathcal{O}_K/P = \mathbb{F}_{p^k}$, $D_{Q/P} = D$, $I_{Q/P} = I \triangleleft D$.

If $n \mid f_{Q/P}$ let $\psi_n \colon D \to GL_1(\mathbb{C}) \cong \mathbb{C}^\times$ be a 1-dimensional representation of D, with $\psi_n(I) = \{1\}$ and $\psi_n(\text{Frob}_{Q/P}) = \zeta_n$, i.e.,

$$\psi_n \colon D \to D/I = \langle \text{Frob}_{Q/P}\rangle \to \mathbb{C}^\times, \text{Frob}_{Q/P} \mapsto \zeta_n.$$

If $n \nmid f_{Q/P}$ set $\psi_n = 0$.

Lemma 2.12. The number of primes of L above P is

$$\langle \mathbb{I}, \operatorname{Res}_D^G \operatorname{Ind}_H^G \mathbb{I} \rangle_D.$$

Proof. $\operatorname{Ind}_H^G \mathbb{I} = \mathbb{C}[H\backslash G]$ so the right-hand side is the number of $H - D$ cosets. □

Lemma 2.13. $n \mid f_{S/P}$ if and only if $\operatorname{Res}^D_{D_{Q/S}} \psi_n = \mathbb{I}$. This is also equivalent to $\langle \operatorname{Res}^D_{D_{Q/S}} \psi_n \rangle_{D_{Q/S}} = 1$.

Proof. If $n \nmid f_{Q/P}$ then $n \nmid f_{S/P}$ by multiplicity of f. Assume $n \mid f_{Q/P}$. If $g \in D$ acts on $\mathcal{O}_F/Q$ as $g(x) = x^{(p^k)^t}$ then $\psi_n(g) = \zeta_n^t$ so $\operatorname{Res}^D_{D_{Q/S}} \psi_n = \mathbb{I}$ if and only if all $g \in D_{Q/S}$ fix $\mathbb{F}_{p^{kn}}$ if and only if

$$\mathcal{O}_L/S = (\mathcal{O}_F/Q)^{D_{Q/S}} \supset \mathbb{F}_{p^{kn}},$$

using Theorem 2.4, if and only if $n \mid f_{S/P}$. □

Proposition 2.14. The number of primes R of L above P with $n \mid f_{R/P}$ is

$$\langle \psi_n, \operatorname{Res}_D^H \operatorname{Ind}_H^G \mathbb{I} \rangle.$$

Proof. If $n \nmid f_{Q/P}$ the result is clear, so assume $n \mid f_{Q/P}$.

Let $X = \{x_1, \ldots, x_n\}$ be a set of representatives of $H - D$ double cosets, so X bijects with the primes in L above P via the map sending x to the prime of L below $x(Q)$, by Corollary 2.8.

Note that $\psi_n^x \colon D_{x(Q)} \to \mathbb{C}^\times$ satisfies the definition of ψ_n for the prime $x(Q)$. By Lemma 2.13, the number of primes R of L above P with $n \mid f_{R/P}$ is

$$\begin{aligned}
\sum_{x \in X} \langle \operatorname{Res}^{xDx^{-1}}_{H \cap xDx^{-1}} \psi_n^x, \operatorname{Res}^H_{H \cap xDx^{-1}} \mathbb{I} \rangle &= \sum_{x \in X} \langle \operatorname{Ind}^H \operatorname{Res}_{H \cap xDx^{-1}} \psi_n^x, \mathbb{I} \rangle \\
&= \langle \bigoplus \operatorname{Ind}^H \operatorname{Res}_{H \cap xDx^{-1}} \psi_n^x, \mathbb{I} \rangle_H \\
&= \langle \operatorname{Res}_H^G \operatorname{Ind}_D^G \psi_n, \mathbb{I} \rangle_H \\
&= \langle \psi_n, \operatorname{Res}_D^G \operatorname{Ind}_H^G \mathbb{I} \rangle
\end{aligned}$$

using Frobenius reciprocity and Mackey's formula. □

Chapter 3

L-Series

We will prove the following statements.

(i) If $(a, N) = 1$ then there exists infinitely many primes p with $p \equiv a \pmod{N}$.
(ii) If $f(X) \in \mathbb{Z}[X]$ is monic and $f(X) \pmod{p}$ has a root for all primes p then $f(X)$ is irreducible.

Definition. An *(ordinary) Dirichlet Series* is a series

$$f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

with $a_n \in \mathbb{C}, s \in \mathbb{C}$ and we write $s = \sigma + it$.

3.1 Convergence Properties

Lemma 3.1 (Abel's Lemma)**.**

$$\sum_{n=N}^{M} a_n b_n = \sum_{n=N}^{M-1} \left(\sum_{k=N}^{n} a_k \right) (b_n - b_{n+1}) + \left(\sum_{k=N}^{M} a_k \right) b_M.$$

Proof. Elementary rearrangement. □

Proposition 3.2. Let $\lambda_n \to \infty$ be an increasing sequence of positive reals. If the series

$$f(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$$

converges for $s = s_0$ it converges uniformly in every domain of the form $\Re(s) > \Re(s_0)$, $-A \leq \arg(s - s_0) \leq A$ for $0 < A < \frac{\pi}{2}$. In particular, it converges for $\Re(s) > \Re(s_0)$ and defines an analytic function there.

Proof. The second statement follows from the first, since a uniform limit of analytic functions is analytic. For the first statement, WMA $s_0 = 0$ (by setting $s' = s - s_0$, $a'_n = e^{-\lambda_n s_0} a_n$). Let $\varepsilon > 0$. Now by assumption $\sum a_n$ converges, so there exists N_0 such that for all $N, M \geq N_0$

$$\left| \sum_{n=N}^{M} a_n \right| \leq \varepsilon.$$

Thus we have

$$\begin{aligned}\left|\sum_{n=N}^{m} a_n e^{-\lambda_n s}\right| &= \left|\sum_{n=N}^{M-1}\left(\sum_{k=N}^{n} a_k\right)(e^{-\lambda_n s} - e^{-\lambda_{n+1} s}) + \left(\sum_{k=N}^{M} a_k\right)e^{-\lambda_M s}\right| \\ &\leq \varepsilon \sum_{n=N}^{M-1} |e^{-\lambda_n s} - e^{-\lambda_{n+1} s}| + \varepsilon\end{aligned}$$

Note that

$$\begin{aligned}|e^{-\alpha s} - e^{-\beta s}| &= \left|s\int_\alpha^\beta e^{-xs}\, dx\right| \\ &\leq |s|\int_\alpha^\beta |e^{-xs}|\, dx \\ &= |s|\int_\alpha^\beta e^{-x\sigma}\, dx \\ &= \frac{|s|}{\sigma}(e^{-\alpha\sigma} - e^{-\beta\sigma})\end{aligned}$$

for $0 < \alpha < \beta$ and where $\sigma = \Re(s)$. Hence

$$\begin{aligned}\left|\sum_{n=N}^{M} a_n e^{-\lambda_n s}\right| &\leq \varepsilon\frac{|s|}{\sigma}\sum_{n=N}^{M-1}\left(e^{-\lambda_n\sigma} - e^{-\lambda_{n+1}\sigma}\right) + \varepsilon \\ &= \varepsilon\left(\frac{|s|}{\sigma}(e^{-\lambda_N\sigma} - e^{-\lambda_M\sigma}) + 1\right) \\ &\leq \varepsilon\left(\frac{|s|}{\sigma} + 1\right) \\ &\leq \varepsilon(K+1)\end{aligned}$$

for some $K > 0$ independent of s, by choice of our domain. □

Proposition 3.3. Let $\lambda_n \to \infty$ be an increasing sequence of positive reals. Suppose a_n are real and positive for all n. Suppose the series

$$f(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$$

converges on $\Re(s) > R \in \mathbb{R}$, and the series has an analytic continuation to a neighbourhood of R. Then it converges for $\Re(s) > R - \varepsilon$ for some $\varepsilon > 0$.

Proof. We may assume that $R = 0$. Then f is analytic on $\Re(s) > 0$ and on a disc around 0, so analytic on a disc of radius $1 + \varepsilon$ around $s = 1$.

Therefore, its Taylor series around 1 converges on $-\varepsilon$.

$$f(-\varepsilon) = \sum_{k=0}^{\infty} \frac{1}{k!}(-1)^k(1+\varepsilon)^k f^{(k)}(1)$$

converges and

$$f^{(k)}(s) = \sum_{n=1}^{\infty} a_n(-\lambda_n)^k e^{-\lambda_n s}$$

for $\Re(s) > 0$, where term-by-term differentiation is justified by local uniform convergence. So

$$(-1)^k f^{(k)}(1) = \sum_{n=1}^{\infty} a_n \lambda_n^k e^{-\lambda_n}$$

is a convergent series with positive terms. Hence

$$\begin{aligned} f(-\varepsilon) &= \sum_{k=0}^{\infty} \frac{1}{k!}(-1)^k(1+\varepsilon)^k \sum_{n=1}^{\infty} a_n(-1)^k \lambda_n^k e^{-\lambda_n} \\ &= \sum_{k,n} a_n \lambda_n^k e^{-\lambda_n} \frac{1}{k!}(1+\varepsilon)^k \end{aligned}$$

is a convergent series with positive terms, so a rearrangement of terms is possible,

$$\begin{aligned} &= \sum_{n=1}^{\infty} a_n e^{-\lambda_n} e^{\lambda_n(1+\varepsilon)} \\ &= \sum_{n=1}^{\infty} a_n e^{\lambda_n \varepsilon}. \end{aligned}$$

The right-hand side is a convergent series so the series expression of f at $-\varepsilon$ converges, and hence by Proposition 3.2 on $\Re(s) > -\varepsilon$ as well. □

Proposition 3.4. (i) If a_n are bounded then the series $\sum \frac{a_n}{n^s}$ converges absolutely for $\Re(s) > 1$.

(ii) If the partial sums $\sum_{n=N}^{M} a_n$ are bounded then the series above converges on $\Re(s) > 0$.

Proof. (i) $\sum \frac{1}{n^x}$ converges for $x > 1$, x real.

(ii) Exercise using Abel's Lemma. (First reduce to $s \in \mathbb{R}$, by Proposition 3.2.) □

3.2 Dirichlet L-Functions

Definition. Let $N \geq 1$ be an integer and let

$$\psi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$$

be a group homomorphism. Extend ψ to a function $\psi\colon \mathbb{Z} \to \mathbb{C}$

$$\psi(n) = \begin{cases} \psi(n \mod N) & (n, N) = 1 \\ 0 & \text{otherwise} \end{cases}.$$

Such a function is called a *Dirichlet character* modulo N. Its *L-series*, or *L-Function*, is

$$L_N(\psi, s) = \sum_{n=1}^{\infty} \psi(n) n^{-s}.$$

Remark. (i) $\psi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is often referred to as a Dirichlet character.

(ii) Note that $\psi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is a 1-dimensional representation of $(\mathbb{Z}/N\mathbb{Z})^\times$. Number theorists have the habit of calling 1-dimensional representations characters.

Lemma 3.5. Let ψ be a Dirichlet character modulo N. Then the following hold:

(i) $\psi(a+N) = \psi(a)$, i.e., ψ is periodic.

(ii) $\psi(ab) = \psi(a)\psi(b)$, i.e., ψ is strictly multiplicative.

(iii) The L-series of ψ converges absolutely on $\Re(s) > 1$ and there it satisfies

$$L_N(\psi, s) = \prod_{p \text{ primes}} \frac{1}{1 - \psi(p)p^{-s}}.$$

Remark. This expression is called the *Euler product* for ψ.

Proof. (i) ✓

(ii) ✓

(iii) The coefficients of $L_N(\psi, s)$ are $\psi(n)$ so are bounded, hence by Proposition 3.4 (i) we have absolute convergence on $\Re(s) > 1$. For $\Re(s) > 1$,

$$\begin{aligned}\sum_{n=1}^{\infty} \psi(n)n^{-s} &= \prod_{p \text{ prime}} (1 + \psi(p)p^{-s} + \psi(p)^2p^{-2s} + \cdots) \\ &= \prod_{p \text{ prime}} \frac{1}{1 - \psi(p)p^{-s}}\end{aligned}$$

where the expansion is justified by absolute convergence. □

Remark. $\psi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ with $\psi(n) = 1$ for all $n \in (\mathbb{Z}/N\mathbb{Z})^\times$ gives the trivial Dirichlet character modulo N. In this case,

$$L_N(\psi, s) = \zeta(s) \prod_{\substack{p|N \\ p \text{ prime}}} (1 - p^{-s})$$

where $\zeta(s)$ is the Riemann zeta function.

Theorem 3.6. Let $N \geq 1$ and $\psi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$.

(i) If ψ is the trivial character then $L_N(\psi, s)$ has an analytic continuation to $\Re(s) > 0$ except for a simple pole at $s = 1$.

(ii) If ψ is non-trivial then $L_N(\psi, s)$ is analytic on $\Re(s) > 0$.

Proof. (i) Follows from the last remark and that $\zeta(s)$ has an analytic continuation to $\mathbb{C}$, except for a simple pole at $s = 1$.

(ii)

$$\begin{aligned}\sum_{n=A}^{A+N-1} \psi(n) &= \sum_{n \in (\mathbb{Z}/N\mathbb{Z})^\times} \psi(n) \\ &= \langle \psi, \mathbb{I} \rangle \\ &= 0\end{aligned}$$

as $\psi \neq \mathbb{I}$. So the sums $\sum_{n=A}^{B} \psi(n)$ are bounded, and the result follows from Proposition 3.4 (ii). □

Theorem 3.7. Let ψ be a non-trivial Dirichlet character modulo N. Then

$$L_N(\psi, 1) \neq 0.$$

Proof. Let

$$\zeta_N(s) = \prod_{\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} L_N(\chi, s)$$

for $\Re(s) > 1$. Suppose that $L_N(\psi, 1) = 0$. Then $\zeta_N(s)$ has an analytic continuation to $\Re(s) > 0$ by Theorem 3.6, the pole from $L_N(\mathbb{I}, s)$ having been killed by the zero of $L_N(\psi, s)$ at $s = 1$.

On $\Re(s) > 1$, $\zeta_N(s)$ has the absolute convergent Euler product

$$\begin{aligned}\zeta_N(s) &= \prod_{\chi} \prod_{p \text{ prime}} \frac{1}{1 - \chi(s)p^{-s}} \\ &= \prod_{\substack{p \text{ prime} \\ p \nmid N}} \prod_{\chi} \frac{1}{1 - \chi(p)p^{-s}}.\end{aligned}$$

Now

$$\prod_{\chi}(1 - \chi(p)X) = (1 - X^{f_p})^{\phi(N)/f_p}$$

where f_p is the order of p modulo N and ϕ is the Euler totient function.

[Indeed, $\chi(p)$ takes values that are f_pth roots of unity, each occurring the same number of times; finally

$$\prod_{i=0}^{f_p - 1} (1 - \zeta_{f_p}^i X) = 1 - X^{f_p}.$$

]

So on $\Re(s) > 1$, $\zeta_N(s)$ has Dirichlet series obtained by expanding

$$\zeta_N(s) = \prod_{p \nmid N} (1 + p^{-f_p s} + p^{-2f_p s} + p^{-3f_p s} + \cdots)^{\phi(N)/f_p}.$$

By Proposition 3.3, as this series has positive coefficients and an analytic continuation to $\Re(s) > 0$ it must converge in that region.

But the above series dominates

$$\prod_{p \nmid N} (1 + p^{-\phi(N)s} + p^{-2\phi(N)s} + p^{-3\phi(N)s} + \cdots)$$

for $s \in \mathbb{R}$, $s \geq 0$, which is the Dirichlet series of $L_N(\mathbb{I}, \phi(N)s)$ which diverges when $s = \frac{1}{\phi(N)}$. Contradiction. □

Example. Let $N = 10$, so $\mathbb{Z}/N\mathbb{Z})^\times = \{1, 3, 7, 9\} \cong C_4$, take $\psi\colon (\mathbb{Z}/10\mathbb{Z})^\times \to \mathbb{C}^\times$,

$$\psi(1) = 1, \qquad \psi(3) = i, \qquad \psi(7) = -i, \qquad \psi(9) = 1.$$

Then

$$L_1 0(\psi, s) = 1 + \frac{i}{3^s} - \frac{i}{7^s} - \frac{1}{9^s} + \frac{1}{11^s} + \frac{i}{13^s} - \frac{i}{17^s} - \frac{1}{19^s} + \cdots.$$

3.3 Primes in Arithmetic Progression

Proposition 3.8. Let ψ be a Dirichlet character modulo N.

(i) The Dirichlet series

$$\sum_{\substack{\text{primes } p \\ n \geq 1}} \frac{\psi(p)^n}{n} p^{-ns}$$

converges absolutely on $\Re(s) > 1$ to an analytic function, and defines (a branch of) $\log L_N(\psi, s)$ there.

(ii) If ψ is a non-trivial character then

$$\sum \frac{\psi(p)^n}{n} p^{-ns}$$

is bounded as $s \to 1$. If $\psi = \mathbb{I}$ then

$$\sum \frac{\psi(p)^n}{n} p^{-ns} \sim \log \frac{1}{s-1}$$

as $s \to 1$.

Proof. (i) The series has bounded coefficients so converges absolutely on $\Re(s) > 1$ to an analytic function by Proposition 3.4 (i).
Take a branch of the logarithm with

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$$

for small x. Then

$$\log L_N(\psi, s) = \log \prod_p \frac{1}{1 - \psi(p)p^{-s}}.$$

By continuity of the logarithm and convergence of the Euler product,

$$\begin{aligned} &= \sum_p \log \frac{1}{1 - \psi(p)p^{-s}} \\ &= \sum_p \left(\psi(p)p^{-s} + \frac{\psi(p)^2 p^{-2s}}{2} + \frac{\psi(p)^3 p^{-3s}}{3} + \cdots \right) \\ &= \sum_{p,n} \frac{\psi(p)^n}{n} p^{-ns}. \end{aligned}$$

(ii) Follows from Theorem 3.7. If ψ is non-trivial then $L(\psi, s)$ converges to a non-zero value as $s \to 1$, hence its logarithm is bounded near 1.
$L(\mathbb{I}, s)$ has a simple pole at $s = 1$, hence $L(\mathbb{I}, s) \sim \frac{\lambda}{1-s}$, so $\log L(\mathbb{I}, s) \sim \frac{1}{s-1}$ as $s \to 1$. □

Corollary 3.9. If ψ is non-trivial then $\sum_{p \text{ prime}} \psi(p)p^{-s}$ is bounded as $s \to 1$. If ψ is trivial then $\sum \psi(p)p^{-s} = \sum_{p \nmid N} p^{-s} \sim \log\left(\frac{1}{s-1}\right)$ as $s \to 1$. In particular, it converges to ∞.

Proof.

$$\sum_p \psi(p)p^{-s} = \log L_N(\psi, s) - \sum_{\substack{n\geq 2\\ p \text{ prime}}} \frac{\psi(p)^n}{n} p^{-ns}$$

so it suffices to prove that the last term is bounded on $\Re(s) > 1$. But on $\Re(s) > 1$,

$$\begin{aligned}
\Big| \sum_{\substack{n\geq 2\\ p \text{ prime}}} \frac{\psi(p)^n}{n} p^{-ns} \Big| &\leq \sum_{\substack{n\geq 2\\ p \text{ prime}}} \Big| \frac{\psi(p)^n}{n} p^{-ns} \Big| \\
&\leq \sum_{\substack{p\nmid N\\ n\geq 2}} \Big| \frac{1}{p^{ns}} \Big| \\
&\leq \sum_p \frac{1}{|p^s|\big(|p^s| - 1\big)} \\
&\leq \sum_p \frac{1}{p(p-1)} \\
&\leq 2 \sum_{k\in\mathbb{N}} \frac{1}{k^2} < \infty
\end{aligned}$$

□

Theorem 3.10 (Dirichlet's Theorem on Primes in Arithmetic Progressions)**.** Let $a, N \geq 1$ be coprime. Then there are infinitely many primes p with $p \equiv a \pmod N$. Moreover, if P_a is the set of these primes then

$$\sum_{p\in P_a} \frac{1}{p^s} \sim \frac{1}{\phi(N)} \log \frac{1}{s-1}$$

as $s \to 1$.

Proof. Notice that the first statement follows from the second. Let C_a be the class function $C_a \colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$,

$$C_a(n) = \begin{cases} 1 & n = a \\ 0 & n \neq a \end{cases}.$$

So

$$\sum_{p\in P_a} \frac{1}{p^s} = \sum_{p \text{ prime}} C_a(p)p^{-s}.$$

Now write C_a as a sum of Dirichlet characters.

$$\begin{aligned}
\langle C_a, \chi\rangle &= \frac{1}{\phi(N)} \sum_{n\in(\mathbb{Z}/N\mathbb{Z})^\times} C_a(n)\overline{\chi(n)} \\
&= \frac{\overline{\chi(a)}}{\phi(N)}.
\end{aligned}$$

Hence $C_a = \sum_\chi \frac{\overline{\chi(a)}}{\phi(N)}\chi$. So

$$\sum_{p\in P_a} \frac{1}{p^s} = \sum_\chi \frac{\overline{\chi(a)}}{\phi(N)} \sum_{p \text{ prime}} \chi(p)p^{-s}.$$

Each term on the right-hand side is bounded as $s \to 1$ except for the contribution from $\chi = \mathbb{I}$, so

$$\sum_{p \in P_a} \frac{1}{p^s} \sim \frac{1}{\phi(N)} \sum_{p \nmid N} p^{-s} \sim \frac{1}{\phi(N)} \log \frac{1}{s-1}$$

as $s \to 1$ by Corollary 3.9. □

3.4 Dirichlet Characters

Recall that

$$\begin{aligned} (\mathbb{Z}/N\mathbb{Z})^\times &\xrightarrow{\sim} \mathrm{Gal}\big(\mathbb{Q}(\zeta_N)/\mathbb{Q}\big) \\ a &\mapsto \sigma_a & \sigma_a(\zeta_N) &= \zeta_N^a \\ p &\mapsto \sigma_p & \sigma_p(\zeta_N) &= \zeta_N^p \end{aligned}$$

If Q is a prime of $\mathbb{Q}(\zeta_N)$ above $p \nmid N$ then $\sigma_P = \mathrm{Frob}_{Q/P}$.

Notation. If F/K is a Galois extension of number fields with $\mathrm{Gal}(F/K)$ abelian, and P is a prime of K unramified in F/K, write $\mathrm{Frob}_P \in \mathrm{Gal}(F/K)$ for the Frobenius element of any prime above P, independent of Q above P as the decomposition groups are conjugate, and $I = 1$ as P is unramified.

Theorem 3.11 (Hecke, 1920, *Class Field Theory*)**.** Let F/K be a Galois extension of number fields with $\mathrm{Gal}(F/K)$ abelian, and $\psi\colon \mathrm{Gal}(F/K) \to \mathbb{C}^\times$ a homomorphism. Then

$$L_*(\psi, s) = \prod_{\substack{p \text{ primes of } K \\ \text{unramified in } F/K}} \frac{1}{1 - \psi(\mathrm{Frob}_P) N(P)^{-s}}$$

has an analytic continuation to $\mathbb{C}$, except for a simple pole at $s = 1$ when $\psi = \mathbb{I}$.

Proof. Omitted. □

Remark. When $K = \mathbb{Q}$, $F = \mathbb{Q}(\zeta_N)$ this recovers Theorem 3.6, and more.

3.5 Artin L-Functions

Notation. If $I \leq D$ are finite groups, ρ a D-representation, write

$$\rho^I = \{v \in \rho : \forall g \in I \quad gv = v\}$$

for the subspace of I-invariant vectors.

Remark. If $I \lhd D$ then ρ^I is a D-subrepresentation. If $v \in \rho^I$, $g \in D$, $i \in I$ then

$$i(gv) = g(i'v) = gv$$

for some $i' \in I$, so $gv \in \rho^I$.

Definition. Let F/K be a Galois extension of number fields, let ρ be a $\mathrm{Gal}(F/K)$-representation. Let P be a prime of K, and choose Q a prime of F above K, choose Frob_P to be an element of $D_{Q/P}$ which in $D_{Q/P}/I_{Q/P}$ is $\mathrm{Frob}_{Q/P}$, i.e., Frob_P acts on the residue field as Frobenius. Then the *local polynomial* of ρ at P is

$$\begin{aligned} P_P(\rho, T) &= P_P(F/K, \rho, T) \\ &= \det\bigl(1 - T\,\mathrm{Frob}_P \mid \rho^{I_P}\bigr) \end{aligned}$$

where $I_P = I_{Q/P}$ and the right-hand side is $\det(1 - T\,\mathrm{Frob}_P)$ acting at $\bigl(\mathrm{Res}^{\mathrm{Gal}\,F/K}_{D_{Q/P}}\,\rho\bigr)^{I_P}$.

Lemma 3.12. *$P_P(\rho, T)$ is independent of the choice of Q and Frob_P.*

Proof. For fixed Q, independence of choice of Frob_P is clear: another choice differs by an element of $I_{Q/P}$ which acts as the identity at $\rho^{I_{Q/P}}$.

If $Q' = gQ$ is another prime, $g \in \mathrm{Gal}(F/K)$, then we can take Frob'_P for Q' to be $g\,\mathrm{Frob}_P\,g^{-1}$ and observe that eigenvalues (with multiplicities) of $g\,\mathrm{Frob}_P\,g^{-1}$ on $\rho^{gI_Pg^{-1}}$ agree with eigenvalues of Frob_P on ρ^{I_P}, so have the same minimal polynomial and hence give the same local factors. □

Definition. Let F/K be a Galois extension of number fields, and ρ be a $\mathrm{Gal}(F/K)$-representation. The *Artin L-function* of ρ is defined by the Euler product

$$L(F/K, \rho, s) = L(\rho, s) = \prod_{K \text{ prime of } K} \frac{1}{P_P(\rho, N(P)^{-s}}.$$

The polynomial $P_P(\rho, T)$ has the form $1 - (aT + bT^2 + \cdots + zT^{\dim \rho^I})$, so we can write

$$\begin{aligned} \frac{1}{P_P(\rho, T)} &= 1 + (aT + bT^2 + \cdots) + (aT + bT^2 + \cdots)^2 + \cdots \\ &= 1 + a_P T + a_{P^2} T^2 + a_{P^3} T^3 + \cdots . \end{aligned}$$

Formally, substituting this into the above product gives the series expression (Artin L-series)

$$\begin{aligned} L(\rho, s) &= \prod_P (1 + a_P N(P)^{-s} + a_{P^2} N(P)^{-2s} + \cdots) \\ &= \sum_{\substack{(0) \neq N \subset \mathcal{O}_K \\ N \text{ ideal}}} a_N N(N)^{-s} \end{aligned}$$

for some $a_N \in \mathbb{C}$.

Note that grouping ideals with equal norm yields an expression for $L(\rho, s)$ as an ordinary Dirichlet series.

Lemma 3.13. *The L-series expression for $L(\rho, s)$ agrees with the Euler product on $\Re(s) > 1$, where both converge absolutely to an analytic function.*

Proof. It suffices to check that the double series

$$\prod_P (1 + a_P N(P)^{-s} + a_{P^2} N(P)^{-2s} + \cdots)$$

converges absolutely on $\Re(s) > 1$ — this justifies both the Euler product and the series expressions on $\Re(s) > 1$, then the analyticity follows from the expression of $L(\rho, s)$ as an ordinary Dirichlet series by Proposition 3.2.

The polynomial $P_P(\rho, T)$ factorises over $\mathbb{C}$ as

$$P_P(\rho, T) = (1 - \lambda_1 T) \cdots (1 - \lambda_k T)$$

with $|\lambda_i| = 1$ and $k \leq \dim \rho$. So the coefficients of

$$\frac{1}{P_P(\rho, T)} = \frac{1}{\prod_i (1 - \lambda_i T)} = 1 + a_P T + a_{P^2} T^2 + \cdots$$

are bounded in absolute value by those of

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

Hence

$$\prod_{P \text{ prime above } p} \sum_{j \geq 0} |a_{P^j}||N(P)^{-js}| \leq \left(\frac{1}{(1 - p^{-\sigma})^{\dim \rho}} \right)^{[K:\mathbb{Q}]}$$

where $\sigma = \Re(s)$ and we note $a_{(1)} = 1$, whence

$$\begin{aligned} \prod_P \sum_{j \geq 0} |a_{P^j}||N(P)^{-js}| &\leq \left(\prod_p \frac{1}{1 - p^{-\sigma}} \right)^{(\dim \rho)[K:\mathbb{Q}]} \\ &= \zeta(s)^{(\dim \rho)[K:\mathbb{Q}]} \end{aligned}$$

as $\Re(s) > 1$. □

Example. (i) Let $K = \mathbb{Q}$, F arbitrary, $\rho = \mathbb{I}$. Then for a prime $P = (p)$ of K, $\rho^{I_P} = \rho$ and Frob_P acts as the identity on ρ^{I_P}. So $P_P(\rho, T) = \det(1 - T|\mathbb{I}) = 1 - T$. Thus $L(\mathbb{I}, s) = \prod_p \frac{1}{1 - p^{-s}} = \zeta(s)$.

(ii) Let K, F be arbitrary, $\rho = \mathbb{I}$. Then

$$L(\mathbb{I}, s) = \prod_P \frac{1}{1 - N(P)^{-s}} = \rho_K(s)$$

the *Dedekind ρ-function* of K.

(iii) Let $K = \mathbb{Q}$, $F = \mathbb{Q}(\zeta_N)$, where N is prime, and ρ 1-dimensional nontrivial. Then

$$L(\rho, s) = L_N(\psi, s)$$

where ψ is the Dirichlet character modulo N defined by $\psi(n) = \rho(\sigma_n)$ where $\sigma_n \in \mathrm{Gal}\big(\mathbb{Q}(\zeta_N)/\mathbb{Q}\big)$ wich $\sigma_n \zeta_N = \zeta_N^n$.

Notation. If $\rho \colon G \to GL_n(\mathbb{C})$ is a representation then write

$$\begin{aligned} \mathrm{Tr}\Big(\sum \lambda_i g_i \;\Big|\; \rho\Big) &= \mathrm{Tr}\Big(\sum \lambda_i \rho(g_i)\Big) = \sum \lambda_i \chi_\rho(g_i), \\ \det\Big(\sum \lambda_i g_i \;\Big|\; \rho\Big) &= \det\Big(\sum \lambda_i \rho(g_i)\Big). \end{aligned}$$

3.6 Properties of Artin L-Functions

Proposition 3.14. Let F/K be a Galois extension of number fields and ρ be a representation of $\mathrm{Gal}(F/K)$.

(i) If τ is another $\mathrm{Gal}(F/K)$-representation then

$$L(\rho \oplus \tau, s) = L(\rho, s)L(\tau, s).$$

(ii) If $N \triangleleft \mathrm{Gal}(F/K)$ and ρ is trivial on N so ρ comes from a representation ρ' of $\mathrm{Gal}(F/K)/N \cong \mathrm{Gal}(F^N/K)$ then

$$L(F/K, \rho, s) = L(F^N/K, \rho', s).$$

(iii) (Artin Formalism) If $\rho = \mathrm{Ind}_H^{\mathrm{Gal}(F/K)} \tau$ for some $H \leq G$, τ an H-representation then

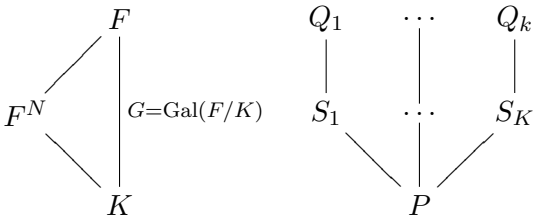
$$L(F/K, \rho, s) = L(F/F^H, \tau, s).$$

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

(i) Observe $(\rho \oplus \tau)^{I_P} = \rho^{I_P} \oplus \tau^{I_P}$.

(ii) Straight from the definition. Observe that Frobenius for F/K projects to Frobenius for F^N/K and similarly for inertia.

(iii) Let $S_1, \ldots, S_k$ be the primes of F^N above P and take Q_i to be a prime of F above S_i, say $Q = Q_1$, $Q_i = x_i Q$ for some $x_i \in \mathrm{Gal}(F/K)$.



It remains to show that

$$\det\bigl(1 - T\,\mathrm{Frob}_{Q/P} \mid (\mathrm{Ind}_H^G \tau)^{I_{Q/P}}\bigr) = \prod_{S_i} \det\bigl(1 - T^{f_{Q_i/P}}\,\mathrm{Frob}_{Q_i/S_i} \mid \tau^{I_{Q_i/S_i}}\bigr).$$

Step 1. Assume there is a unique prime in F above P. Note that it suffices to show the equality when τ is irreducible. Write $\mathrm{Ind}_H^G \tau = \bigoplus_i \sigma_i$, where σ_i are irreducible representations of G.

- If $\tau^{I_{Q/S}} = 0$ then $I_{Q/S}$ acts non-trivially on τ, so by Frobenius reciprocity $I_{Q/P}$ acts non-trivially onσ_i and $\langle \sigma_i, \mathrm{Ind}\,\tau \rangle = \langle \mathrm{Res}\,\sigma_i, \tau \rangle$. Then $\sigma_i^{I_{Q/P}} = 0$ so $(\mathrm{Ind}\,\tau)^{I_{Q/P}} = 0$, and now the result is trivial.
- If $\tau^{I_{Q/S}} \neq 0$ then $I_{Q/S}$ acts trivially on τ, so τ is 1-dimensional, $\tau(I_{Q/S}) = 1$, $\tau(\mathrm{Frob}_{Q/S}) = \zeta_n$, say. So

$$\det\bigl(1 - T\,\mathrm{Frob}_{Q/S} \mid \tau^{I_{Q/S}}\bigr) = 1 - \zeta_n T^f.$$

The σ_i on which $I_{Q/P}$ acts non-trivially have $\sigma_i^{I_{Q/P}} = 0$ so do not contribute. The rest are 1-dimensional, $\sigma_i(I_{Q/P}) = 1$ and $\sigma_i(\mathrm{Frob}_{Q/P}) = \zeta_{n_i}$, say. Observe

$$\mathrm{Frob}_{Q/P}^{f_{S/P}} = \mathrm{Frob}_{Q/S}$$

up to inertia, so by Frobenius reciprocity, for each primitive $(nf_{S_i/P})$th root of unity $\zeta_{nf_{S_i/P}}$, with $\zeta_{nf}^{f_{S_i/P}} = \zeta_n$, exactly one such σ_i occurs in $\mathrm{Ind}_H^G \tau = \bigoplus \sigma_i$.

Therefore,

$$\det\big(1 - \mathrm{Frob}_{Q/P} \;\big|\; (\mathrm{Ind}\,\tau)^{I_{Q/P}}\big) = \prod (1 - \zeta_{nf_{S/P}} T) = 1 - \zeta_n T^{f_{S/P}}.$$

Step 2. General case.

$$\begin{aligned}
P_P(\mathrm{Ind}\,\tau, T) &= \det\big(1 - T\,\mathrm{Frob}_{Q/P} \big| (\mathrm{Res}^G_{D_{Q/P}} \mathrm{Ind}^G_H \tau)^{I_{Q/P}}\big) \\
&= \det\Big(1 - T\,\mathrm{Frob}_{Q/P} \;\Big|\; \Big(\bigoplus_{x_i} \mathrm{Ind}^{D_{Q/P}}_{x_i^{-1}Hx_i \in D_{Q/P}} \mathrm{Res}^{x_i^{-1}Hx_i}_{x_i^{-1}Hx_i \cap D} \tau^{x_i}\Big)^{I_{Q/P}}\Big) \\
&= \prod_{S_i} \det\Big(1 - T\,\mathrm{Frob}_{Q/P} \;\Big|\; \Big(\mathrm{Ind}^{D_{Q/P}}_{x_i^{-1} D_{Q_i/S_i} x_i} \mathrm{Res}_{x_i^{-1} D_{Q_i/S_i} x_i} \tau^{x_i}\Big)^{I_{Q/P}}\Big) \\
&= \prod_{S_i} \det\Big(1 - T\,\mathrm{Frob}_{Q/P} \;\Big|\; \Big(\mathrm{Ind}^{D_{Q_i/P}}_{D_{Q_i/S_i}} \mathrm{Res}^H_{D_{Q_i/S_i}} \tau\Big)^{I_{Q_i/P}}\Big)
\end{aligned}$$

hence, by Step 1,

$$\begin{aligned}
&= \prod_{S_i} \det\Big(1 - T^{f_{S_i/P}}\,\mathrm{Frob}_{Q_i/P_i} \;\Big|\; \big(\mathrm{Res}^H_{D_{Q_i/S_i}} \tau\big)^{I_{Q_i/S_i}}\Big) \\
&= \prod_{S_i} P_{S_i}(\tau, T^{f_{S_i/P}})
\end{aligned}$$

□

Proposition 3.15 (Artin's Theorem)**.** Let G be a finite group, ρ a G-representation. Then there are cyclic subgroups $H_i, H_j' \leq G$ and 1-dimensional representations τ_i, τ_j' of H_i, H_j' such that

$$\rho^{\oplus n} \oplus \bigoplus_i \mathrm{Ind}^G_{H_i} \tau_i = \bigoplus_j \mathrm{Ind}^G_{H_j'} \tau_j'.$$

If $\langle \rho, \mathbb{I} \rangle = 0$ then τ_i can be chosen to be non-trivial.

Proof. Slightly non-trivial exercise. □

Theorem 3.16 (Artin)**.** Let F/K be a Galois extension of number fields and ρ a representation of $\mathrm{Gal}(F/K)$. Then there exists $n \geq 1$ such that $L(\rho, s)^n$ admits a meromorphic continuation to $\mathbb{C}$, analytic and non-zero at $s = 1$ if $\langle \rho, \mathbb{I} \rangle = 0$.

Proof. Proposition 3.15 and Artin Formalism reduce the problem to showing that $L(\tau, s)$ has analytic continuation to $\mathbb{C}$ when τ is 1-dimensional, except possibly a pole at $s = 1$ when $\tau = \mathbb{I}$.

This is true by Hecke's Theorem and the fact that only finitely many primes ramify in any extension of number fields, and $L(\tau, s)$ is non-zero at $s = 1$. □

Corollary 3.17. If ρ is irreducible and non-trivial then $L(\rho, s)$ is bounded and non-zero near $s = 1$.

Proof. Observe if F/K is cyclic then this is true by Theorem 3.11. □

Conjecture. If ρ is irreducible and non-trivial then $L(\rho, s)$ has analytic continuation to $\mathbb{C}$.

Remark. Theorem 3.16 implies that $L(\rho, s)^n$ is meromorphic. A theorem of Brauer states that $L(\rho, s)$ is meromorphic.

3.7 Density Theorems

Definition. Let S be a set of prime numbers. Then S has *Dirichlet density* α if

$$\frac{\sum_{p \in S} \frac{1}{p^s}}{\log \frac{1}{s-1}} \to \alpha$$

as $s \to 1$ from above in $\mathbb{R}$.

Example. By Dirichlet's Theorem (Theorem 3.10), the set of all primes has density 1 and $S_{a,N} = \{p : p \equiv a \pmod N\}$ has density $1/\phi(N)$ for a and N coprime.

Notation. For $F/\mathbb{Q}$ Galois and P unramified in F, write $\mathrm{Frob}_P \in \mathrm{Gal}(F/\mathbb{Q})$ for the Frobenius element $\mathrm{Frob}_{Q/P}$ of some Q above P. Note that Frob_P lies in a well-defined conjugacy class of $\mathrm{Gal}(F/\mathbb{Q})$, because $\mathrm{Frob}_{Q'/P} = x \,\mathrm{Frob}_{Q/P}\, x^{-1}$ where $Q' = xQ$ for some $x \in \mathrm{Gal}(F/\mathbb{Q})$.

Example. $F = \mathbb{Q}(\zeta_N)$ and $\sigma_a \in \mathrm{Gal}(F/\mathbb{Q})$ with $\sigma_a(\zeta_N) = \zeta_N^a$ then, for $p \nmid N$, $\mathrm{Frob}_P = \sigma_a$ if and only if $p \equiv a \pmod N$, because $\mathrm{Frob}_P(\zeta_N) = \zeta_N^p$.

So by Dirichlet's Theorem, the set $S_{N,\sigma} = \{p \text{ unramified in } \mathbb{Q}(\zeta_N)/\mathbb{Q} : \mathrm{Frob}_p = \sigma\}$ has Dirichlet density $1/\phi(N) = 1/|\mathrm{Gal}\big(\mathbb{Q}(\zeta_N)/\mathbb{Q}\big)|$ for every $\sigma \in \mathrm{Gal}\big(\mathbb{Q}(\zeta_N)/\mathbb{Q}\big)$.

Theorem 3.18 (Chebotarev's Density Theorem)**.** Let $F/\mathbb{Q}$ be a finite Galois extension and $\mathcal{C}$ a conjugay class in $G = \mathrm{Gal}(F/\mathbb{Q})$. Then the set $S_{\mathcal{C}} = \{p \text{ unramified in } F/\mathbb{Q} : \mathrm{Frob}_p \in \mathcal{C}\}$ has Dirichlet density $|\mathcal{C}|/|G|$.

Corollary 3.19. Let $f(X) \in \mathbb{Z}[X]$ be monic and irreducible. Then the set of primes p such that $f(X) \pmod p$ factorises into irreducible polynomials of degrees $d_1, \ldots, d_n$ has Dirichlet density

$$\frac{|\{g \in \mathrm{Gal}(f) \text{ with cycle type } (d_1, \ldots, d_n) \text{ in the action on roots}\}|}{|\mathrm{Gal}(f)|}.$$

Proof. $f(X) \pmod p$ has a repeated root in $\bar{\mathbb{F}}_p$ for only finitely many p. For the rest, Frob_p acts as an element of cycle type $(d_1, \ldots, d_n)$ where these are the degrees of the irreducible factors of $f(X) \pmod p$, by Corollary 2.5 and its proof. □

Example. Suppose $f(X)$ is an irreducible quintic with $\mathrm{Gal}(f) = S_5$.

- The set of primes such that $f(X) \pmod p$ is a product of linear factors has density $1/120$.
- The set of primes such that $f(X) \pmod p$ factorises into a cubic and a quadratic has density

$$\frac{1}{|S_5|}|\{\text{elements of the form } (\cdot\cdot)(\cdot\cdot\cdot) \text{ in } S_5\}| = \frac{20}{120} = \frac{1}{6}.$$

Corollary 3.20. If $f(X) \in \mathbb{Z}[X]$ is monic and irreducible with $\deg f(X) \geq 2$ then $f(X) \pmod p$ has no root in $\mathbb{F}_p$ for infinitely many primes p.

Proof. It suffices to prove that there exists a $g \in \mathrm{Gal}(f)$ that fixes no root of $f(X)$. But $\bigcup_{\alpha: f(\alpha)=0} \mathrm{Stab}_{\mathrm{Gal}(f)}(\alpha)$ is smaller than $\mathrm{Gal}(f)$ as each has size $|\mathrm{Gal}(f)|/|\{\alpha : f(\alpha) = 0\}|$ and contains the identity element. □

Proof of Theorem 3.18. (i) By Example Sheet 1 Question 9, only finitely many primes ramify in $F/\mathbb{Q}$. By Corollary 3.17, if $\rho \neq \mathbb{I}$ is an irreducible representation of G then

$$L_*(\rho, s) = \prod_{p \text{ unramified}} P_p(\rho, p^{-s})^{-1}$$

is bounded and bounded away from zero near $s = 1$.

(ii) Write χ_ρ for the character of ρ, which is irreducible, and set

$$f_\rho(s) = \sum_{p \text{ unramified}} \chi_\rho(\mathrm{Frob}_p) p^{-s}.$$

Then

$$\begin{aligned}\sum_{p \in S_{\mathcal{C}}} p^{-s} &= \sum_{p \text{ unramified}} \mathcal{C}_c(\mathrm{Frob}_p) p^{-s} \\ &= \sum_{\rho \text{ irreducible}} \langle \mathcal{C}_c, \chi_\rho \rangle f_\rho(s) \\ &= \frac{|\mathcal{C}|}{|G|} f_{\mathbb{I}}(s) + \sum_{\rho \neq \mathbb{I}} \langle \mathcal{C}_c, \chi_\rho \rangle f_\rho(s)\end{aligned}$$

where $\mathcal{C}_c(g)$ is 1 if $g \in \mathcal{C}$ and 0 otherwise. Now $f_{\mathbb{I}}(s) \sim \log\left(\frac{1}{s-1}\right)$ as $s \to 1$ by Theorem 3.10 and the first part, so it suffices to prove that $f_\rho(s)$ is bounded as $s \to 1$ for all irreducible $\rho \neq \mathbb{I}$.

(iii) If p is unramified and $\lambda_1, \ldots, \lambda_d$ are the eigenvalues (with multiplicity) of Frob_p on ρ, then

$$\begin{aligned}\log \frac{1}{P_p(\rho, p^{-s})} &= \log \frac{1}{\prod_i (1 - \lambda_i p^{-s})} \\ &= \sum_i \log \frac{1}{1 - \lambda_i p^{-s}} \\ &= \Big(\sum \lambda_i\Big) p^{-s} + \frac{1}{2}\Big(\sum \lambda_i^2\Big) p^{-2s} + \cdots \\ &= \chi_\rho(\mathrm{Frob}_p) p^{-s} + \frac{1}{2}\chi_\rho(\mathrm{Frob}_p^2) p^{-2s} + \cdots .\end{aligned}$$

The Dirichlet series

$$\sum_{p \text{ unramified}} \sum_{n \geq 1} \frac{\chi_\rho(\mathrm{Frob}_p^n)}{n} p^{-ns}$$

has bounded coefficients, so by Proposition 3.8 and its proof defines an analytic branch of $\log L_*(\rho, s)$ on $\Re(s) > 1$; by the first part, it must be bounded as $s \to 1$ on $\Re(s) > 1$.

□

3.8 Appendix (Local Fields)

Definition. A *place* v in a number field K is an equivalence class of non-trivial absolute values.

There are two types: *Infinite places*, i.e., archimedean absolute values, come from embeddings $K \to \mathbb{R}$ or $K \to \mathbb{C}$ and take

$$|x|_v = \begin{cases} |x| & K \to \mathbb{R} \\ |x|^2 & K \to \mathbb{C} \end{cases}.$$

We note that complex conjugate embeddings give rise to the same absolute values. In fact, this is the only case when two of these embeddings give equivalent absolute values, and these are all the archimedean absolute values on K up to equivalence. The number of infinite places is $r_1 + r_2$.

Finite places, i.e., non-archimedean absolute values, correspond to primes in K as follows. If P is a prime, set $|x|_P = N(P)^{-\mathrm{ord}_P(x)}$ where $\mathrm{ord}_P(x)$ is, for $x \in \mathcal{O}_K$, the power of P in the factorisation of (x) and extend this multiplicatively to K^*. It is a fact that these are inequivalent for different P and give all the non-archimedean absolute values up to equivalence.

Note that $|\cdot|_v$ makes K a metric space and its completion K_v is a complete local field.

Henceforth assume that v is finite.

Example.
- If $K = \mathbb{Q}$ and v corresponds to $P = (p)$ then $|\cdot|_v = |\cdot|_p$ and $K_v = \mathbb{Q}_p$.
- If K is a number field and v corresponds to Q above $p \in \mathbb{Q}$ then $|\cdot|_v$ restricted to $\mathbb{Q}$ is equivalent to $|\cdot|_p$. Therefore, K_v is a finite extension of $\mathbb{Q}$.

3.8.1 Residue fields and ramification

We consider the following setting. Let K be a number field, v a finite place corresponding to Q and K_v its completion. Moreover, let $\mathcal{O}_{K_v}$ be its valuation ring and M_v its unique maximal ideal. Finally, $\mathcal{O}_{K_v}^\times$ is the set of units in $\mathcal{O}_{K_v}$ and $k_v = \mathcal{O}_{K_v}/M_v$ the residue field.

We observe that if $Q \subset M_v$ and $\mathcal{O}_K \subset \mathcal{O}_{K_v}$ then the map

$$\mathcal{O}_K/Q \to \mathcal{O}_{K_v}/M_v = k_v$$

is injective, as it is between fields, and surjective, as every element of K_v can be approximated by an element of K. Thus $\mathcal{O}_K/Q \cong k_v$.

Let L/K be a finite extension of number fields and suppose that R lies above Q with place w corresponding to R. One can check that $|\cdot|_w$ extends $|\cdot|_v$. Then L_w/K_v is a finite extension and, by comparing valuations,

$$e_{R/Q} = e_{w/v}, \qquad f_{R/Q} = f_{w/v}.$$

3.8.2 Galois groups

Suppose that F/K is a Galois extension of number fields and let Q be a prime above P with corresponding places w and v.

If $g \in \mathrm{Gal}(F/K)$ preserves Q, i.e., $g \in D_{Q/P}$, then g preserves $|\cdot|_w$ so g is also a topological automorphism, so g extends to an automorphism of F_w. Therefore, we have a map

$$D_{Q/P} \to \mathrm{Gal}(F_w/K_v)$$

which is clearly injective. The crucial fact is that it is also surjective. This is because $|D_{Q/P}| = e_{Q/P} f_{Q/P} = e_{w/v} f_{w/v} = [F_w : K_v] = |\mathrm{Gal}(F_w/K_v)|$.

We observe also that we have an isomorphism $I_{Q/P} \to I_{w/v}$, as both act trivially on the residue field and have the same size.

3.8.3 Applications

Proposition 3.21 (Proposition 1.22 revisited)**.** If $f(X) \in \mathcal{O}_K[X]$ is Eisenstein with respect to P and α is a root of f, then $K(\alpha)/K$ has degree $\deg(f)$ and P is totally ramified in $K(\alpha)/K$.

Proof. Translate the corresponding fact about local fields. □

Proposition 3.22. Decomposition groups (in number fields) are soluble.

Proof. It agrees with the Galois group of finite extensions of $\mathbb{Q}_p$. (Here $I \triangleleft G$ with G/I cyclic, $I_1 \triangleleft I$ with I/I_1 cyclic and I_1 is a p-group.) □

Example. Suppose we are looking for a tower of extensions $F/\mathbb{Q}(\zeta_3)/\mathbb{Q}$ such that $F/\mathbb{Q}$ is Galois with $\mathrm{Gal}(F/\mathbb{Q}) \cong C_4$. This is impossible.

Proof. First observe that 3 ramifies in $\mathbb{Q}(\zeta_3)/\mathbb{Q}$. Then 3 is totally ramified in $F/\mathbb{Q}$ because the inertia group has to be all of C_4. Considering the completions, $F_v/\mathbb{Q}_3$ is totally ramified and Galois with $\mathrm{Gal}(F_v/\mathbb{Q}_3) \cong C_4$. But this is a totally and tamely ramified extension. Therefore, $\mathrm{Gal}(F_v/\mathbb{Q}_3) \hookrightarrow \mathbb{F}_3^\times$, a contradiction. □