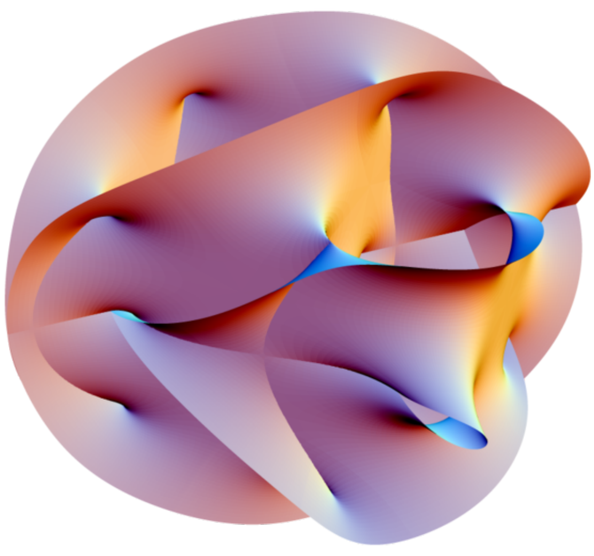
Algebraic Number Theory

Inofficial lecture notes on Algebraic Number Theory given in Michaelmas Term 2010 by Dr. Vladimir Dokchitser at the University of Cambridge

UNIVERSITY OF CAMBRIDGE

Author: **Markus Schepke**
ms946@cam.ac.uk

Sections marked with an asterisk (*) are non-examinable.



Contents

1. Number Fields

1.1. Ring of Integers

Definition (*i*) A *number field* K is a field extension of finite degree over $\mathbb{Q}$. Its *degree* $[K:\mathbb{Q}]$ is its dimension as a $\mathbb{Q}$-vector space. 07.10.

(*ii*) An *algebraic number* α ist an algebraic integer if it is a root of a monic polynomial with integer coefficients. (Equivalently, if the monic minimal polynomial for α over $\mathbb{Q}$ has $\mathbb{Z}$-coefficients).

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

Proposition 1 *(i) $\mathcal{O}_K$ is a (Noetherian) ring.*

(ii) $\operatorname{rank}_{\mathbb{Z}} \mathcal{O}_K = [K:\mathbb{Q}]$, *i. e.* $\mathcal{O}_K \cong \mathbb{Z}^{[K:\mathbb{Q}]}$ *as an abelian group.*

(iii) For every $\alpha \in K$ some integer multiple $n\alpha$ lies in $\mathcal{O}_K$.

Example Let $d \in \mathbb{Z} \setminus \{0,1\}$ be squarefree and ζ_n a primitive n^{th} root of unity.

$$\begin{array}{lllll} K &=& \mathbb{Q}, & \mathcal{O}_K &=& \mathbb{Z} \\ K &=& \mathbb{Q}(\sqrt{d}), & \mathcal{O}_K &=& \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{for } d \equiv 2,3 \mod 4; \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{for } d \equiv 1 \mod 4. \end{cases} \\ K &=& \mathbb{Q}(\zeta_n), & \mathcal{O}_K &=& \mathbb{Z}[\zeta_n] \end{array}$$

Proposition 2 *(i) $\mathcal{O}_K$ is the maximal subring of K which is finitely generated as an abelian group.*

(ii) $\mathcal{O}_K$ is integrally closed in K, i. e. if $f \in \mathcal{O}_K[X]$ is monic and $f(\alpha) = 0$ with $\alpha \in K$, then $\alpha \in \mathcal{O}_K$.

Example In $\mathbb{Z}$, however you factorise integers, you always end up with the same factorisation into irreducible bits, at least up to order and signs:

$$24 = 8 \cdot 3 = 2 \cdot 4 \cdot 3 = 2 \cdot 2 \cdot 2 \cdot 3,$$
$$24 = 6 \cdot 4 = (-2) \cdot (-3) \cdot 4 = (-2) \cdot (-3) \cdot 2 \cdot 2.$$

The ambiguity in signs comes from the units not equal to 1 in $\mathbb{Z}$. The unique factorisation in this form fails in general number fields, e. g. $\mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$:

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

and 2, 3, $1+\sqrt{-5}$, and $1-\sqrt{-5}$ cannot be factorised into non-units. Thus $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. Instead one works with ideals.

1.2. Units

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

Example (*i*) The units in $\mathbb{Q}$ are $\mathbb{Z}^\times = \{\pm 1\}$.

(*ii*) The units in $\mathbb{Q}(i)$ are $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

(*iii*) The units in $\mathbb{Q}(\sqrt{2})$ are $\mathbb{Z}[\sqrt{2}]^\times = \langle -1, 1+\sqrt{2}\rangle = \{\pm(1+\sqrt{2})^n : n \in \mathbb{Z}\}$.

09.10. **Theorem 3** (Dirichlet's Unit Theorem) *Let K be a number field. Then $\mathcal{O}_K^\times$ is finitely generated. More precisely:*

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

where Δ is the (finite) group of roots of unity in K, r_1 is the number of distinct real embeddings $K \hookrightarrow \mathbb{R}$ and r_2 is the number of distinct pairs of complex conjugated embeddings $K \hookrightarrow \mathbb{C}$ with image not contained in $\mathbb{R}$.

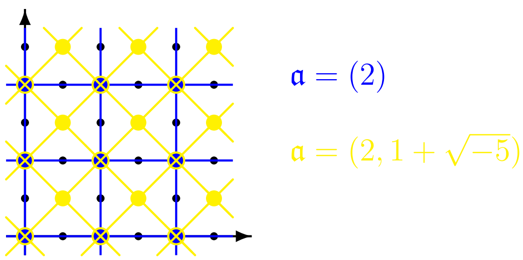
Corollary 4 *The only number fields with finitely many units are $\mathbb{Q}$ and imaginary quadratic fields, i. e. $\mathbb{Q}(\sqrt{-D})$ for an integer $D > 0$.*

1.3. Ideals

Definition Let R be an integral domain. An *ideal* $I \subseteq R$ is a subgroup of $(R, +)$, such that for all $a \in I$ and $r \in R$ holds: $ar \in I$. Notation: $I \lhd R$.

Example (*i*) Let $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$ and $\mathfrak{a} = (17)$ the multiples of 17. Then $\alpha \in \mathfrak{a}$, iff α is a multiple of 17. Multiplication of ideals is just the multiplication of its generators: $(3) \cdot (17) = (51)$.

(*ii*) Let $K = \mathbb{Q}(\sqrt{-5})$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ which is no PID.



An ideal is, in particular, a sublattice of $\mathcal{O}_K$. We will see that it always has finite index in $\mathcal{O}_K$ (so $I \cong \mathbb{Z}^{[K:\mathbb{Q}]}$).

Theorem 5 (Unique factorisation of ideals) *Let K be a number field. Every non-zero ideal of $\mathcal{O}_K$ admits a factorisation into prime ideals. This factorisation is unique up to order.*

Definition Let $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_K$ be two ideals. Then $\mathfrak{a}$ divides $\mathfrak{b}$ (written $\mathfrak{a} \mid \mathfrak{b}$) if $\mathfrak{a} \cdot \mathfrak{c} = \mathfrak{b}$ for some ideal $\mathfrak{c} \lhd \mathcal{O}_K$. (Equivalently, if in the prime factorisations $\mathfrak{a} = \mathfrak{p}^{n_1} \cdots \mathfrak{p}^{n_k}$ and $\mathfrak{b} = \mathfrak{p}^{m_1} \cdots \mathfrak{p}^{m_k}$ we have $n_i \leq m_i$ for all i.)

Remark *(i)* For $\alpha, \beta \in \mathcal{O}_K$ we have $(\alpha) = (\beta)$ iff $\alpha = u\beta$ for some $u \in \mathcal{O}_K^\times$.

(ii) For ideals $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_K$ we have $\mathfrak{a} \mid \mathfrak{b}$ iff $\mathfrak{a} \supseteq \mathfrak{b}$ (non-trivial).

(iii) To multiply ideals, just multiply their generators:

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

(iv) To add ideals, combine their generators, e. g.

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

Lemma 6 *Let $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_K$ be two ideals with prime factorisation $\mathfrak{a} = \prod \mathfrak{p}_i^{n_i}$ and $\mathfrak{b} = \prod \mathfrak{p}_i^{m_i}$. Then:*

(i) $\mathfrak{a} \cap \mathfrak{b} = \prod \mathfrak{p}_i^{\max\{n_i, m_i\}}$ *(least common multiple).*

(ii) $\mathfrak{a} + \mathfrak{b} = \prod \mathfrak{p}_i^{\min\{n_i, m_i\}}$ *(greatest common divisor).*

Proof. We will prove this by using part (ii) of the remark.

(i) This is the largest ideal contained in both $\mathfrak{a}$ and $\mathfrak{b}$.

(ii) This is the smallest ideal contained in both $\mathfrak{a}$ and $\mathfrak{b}$. □

Lemma 7 *Let $\alpha \in \mathcal{O}_K \setminus \{0\}$. Then there is $\beta \in \mathcal{O}_K$, such that $\alpha\beta \in \mathbb{Z} \setminus \{0\}$.*

Proof. Let $X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$ be the minimal polynomial of α. Then $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha = -a_0 \in \mathbb{Z} \setminus \{0\}$. So we can take $\beta := \alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1 \in \mathcal{O}_K$. □

Corollary 8 *If $\mathfrak{a} \lhd \mathcal{O}_K$ is a non-zero ideal, then $[\mathcal{O}_K : \mathfrak{a}]$ is finite.*

Proof. Pick $\alpha \in \mathfrak{a} \setminus \{0\}$ and β with $N = \alpha\beta \in \mathbb{Z} \setminus \{0\}$. Then

$$[\mathcal{O}_K : \mathfrak{a}] \leq [\mathcal{O}_K : (\alpha)] \leq [\mathcal{O}_K : (N)] = [\mathcal{O}_K : N\mathcal{O}_K] = |N|^{[K:\mathbb{Q}]} < \infty.$$ □

Definition The *norm* of a non-zero ideal $\mathfrak{a} \lhd \mathcal{O}_K$ is

$$N(\mathfrak{a}) := [\mathcal{O}_K : \mathfrak{a}].$$

Lemma 9 *Let $\alpha \in \mathcal{O}_K \setminus \{0\}$. Then:*

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

Proof. Let $v_1, \dots, v_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$ and write $T_\alpha : K \to K$ for the $\mathbb{Q}$-linear map $T_\alpha(v) = \alpha v$. Then

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

1.4. Ideal Class Group

Definition Let K be a number field. Define an equivalence relation on non-zero ideals of $\mathcal{O}_K$ by

$$\mathfrak{a} \sim \mathfrak{b} \qquad :\Longleftrightarrow \qquad \exists\, \lambda \in K^\times : \mathfrak{a} = \lambda\mathfrak{b}.$$

The *ideal class group* $\mathcal{C}\ell_K$ of K is the set of classes $\{\mathfrak{a} \lhd \mathcal{O}_K : \mathfrak{a} \neq 0\}/\sim$.

Remark (*i*) The ideal class group $\mathcal{C}\ell_K$ is a group, the group structure coming from multiplication of ideals.

(*ii*) The identity is the class of principal ideals.

(*iii*) $\mathcal{O}_K$ is a UFD, iff $\mathcal{C}\ell_K$ is trivial.

Theorem 10 *The ideal class group $\mathcal{C}\ell_K$ is finite.*

Exercise Let $K = \mathbb{Q}(\sqrt{-D})$ with an integer $D > 0$. Show that two ideals have the same class, iff they are homethetic as lattices in $\mathbb{C} \cong \mathbb{R}^2$, i. e. the ideal class shows the shape of the lattice.

1.5. Primes and Modular Arithmetic

12.10. **Definition** A *prime* $\mathfrak{p}$ of a number field K is a non-zero prime ideal of $\mathcal{O}_K$. Its *residue field* is $\mathcal{O}_K/\mathfrak{p}$ ("$\mathbb{F}_\mathfrak{p}$"), its *residue characteristic* is $p = \operatorname{char} \mathcal{O}_K/\mathfrak{p}$. Its (absolute) *residue degree* is $f_\mathfrak{p} = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$.

Lemma 11 *The residue field of a prime is a finite field.*

Proof. Let $\mathfrak{p}$ be a prime. Then $\mathcal{O}_K/\mathfrak{p}$ is an integral domain. Corollary 8 implies that $|\mathcal{O}_K/\mathfrak{p}| = [\mathcal{O}_K : \mathfrak{p}] = N(\mathfrak{p})$ is finite. Thus $\mathcal{O}_K/\mathfrak{p}$ is a field. □

Remark The size of the residue field at $\mathfrak{p}$ is $|\mathcal{O}_K/\mathfrak{p}| = N(\mathfrak{p})$.

Example (*i*) Let $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$, and $\mathfrak{p} = (17)$. Then $\mathcal{O}_K/\mathfrak{p} = \mathbb{Z}/(17) = \mathbb{F}_{17}$.

(*ii*) Let $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$, and $\mathfrak{p} = (2+i)$. Then $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_5$ with representatives $0, i, i+1, 2i, 2i+1$.

(*iii*) Let $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$, and $\mathfrak{p} = (3)$. Then $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_9$ ("$= \mathbb{F}_3[i]$").

(*iv*) Let $K = \mathbb{Q}(\sqrt{d})$ with $d \equiv 2, 3 \mod 4$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Let $\mathfrak{p}$ be a prime of K with residue characteristic p. Then $\mathcal{O}_K/\mathfrak{p}$ is generated by $\mathbb{F}_p$ and the image of $\sqrt{d}$. The latter is a root of $X^2 - d$ over $\mathbb{F}_p$, so $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_p$, if d is a square mod p, and $\mathbb{F}_{p^2}$ otherwise.

Definition If $\mathfrak{a} \lhd \mathcal{O}_K$ is a non-zero ideal, we say $x \equiv y \mod \mathfrak{a}$, if $x - y \in \mathfrak{a}$. E. g.

$$\begin{aligned} 2 &\equiv 9 \mod (7), \\ 3 &\equiv i \mod (2+i). \end{aligned}$$

Theorem 12 (Chinese Remainder Theorem) *Let K be a number field and $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ distinct primes. Then:*

$$\begin{aligned} \mathcal{O}_K/(\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}) &\xrightarrow{\sim} \mathcal{O}_K/\mathfrak{p}_1^{n_1} \times \ldots \times \mathcal{O}_K/\mathfrak{p}_k^{n_k} \qquad \textit{via} \\ x \bmod \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k} &\longmapsto (x \bmod \mathfrak{p}_1^{n_1}, \ldots, x \bmod \mathfrak{p}_k^{n_k}). \end{aligned}$$

Proof. Define

$$\begin{aligned} \psi : \mathcal{O}_K &\longrightarrow \mathcal{O}_K/\mathfrak{p}_1^{n_1} \times \ldots \times \mathcal{O}_K/\mathfrak{p}_k^{n_k} \qquad \text{by} \\ x &\longmapsto (x \bmod \mathfrak{p}_1^{n_1}, \ldots, x \bmod \mathfrak{p}_k^{n_k}). \end{aligned}$$

Then

$$\ker \psi = \{x : x \equiv 0 \mod \mathfrak{p}_i^{n_i} \ \forall\, i\} = \bigcap_i \mathfrak{p}_i^{n_i} \overset{\text{L6}}{=} \prod_i \mathfrak{p}_i^{n_i}.$$

It remains to prove that ψ is surjective. Lemma 6 implies

$$\mathfrak{p}_j^{n_j} + \prod_{i \neq j} \mathfrak{p}_i^{n_i} = \mathcal{O}_K,$$

so there is an $\alpha \in \mathfrak{p}_j^{n_j}$ and $\beta \in \prod_{i \neq j} \mathfrak{p}_i^{n_i}$ with $\alpha + \beta = 1$. Now $\beta \equiv 0 \mod \mathfrak{p}_i^{n_i}$ for all $i \neq j$ and $\beta \equiv 1 \mod \mathfrak{p}_j^{n_j}$. Thus $\operatorname{im} \psi$ contains $\psi(\beta) = (0, \ldots, 0, 1, 0, \ldots, 0)$. This is true for all j, hence ψ is surjective. $\square$

Remark The Chinese Remainder Theorem implies that we can solve any system of congruences

$$\begin{aligned} x &\equiv a_1 \mod \mathfrak{p}_1^{n_1}, \\ &\vdots \\ x &\equiv a_k \mod \mathfrak{p}_k^{n_k}. \end{aligned}$$

This is called the *Weak Approximation Theorem.*

Lemma 13 *Let $\mathfrak{p} \lhd \mathcal{O}$ be a prime ideal.*

(i) $|\mathcal{O}_K/\mathfrak{p}^n| = N(\mathfrak{p})^n$.

(ii) $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}_K/\mathfrak{p}$ *as an* $\mathcal{O}_K$*-module (or abelian group).*

Proof. The second statement implies the first one:

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

By unique factorisation we have $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$, so pick $\pi \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$. Thus $\mathfrak{p}^n \mid (\pi)$, $\mathfrak{p}^{n+1} \nmid (\pi)$ and $(\pi) + \mathfrak{p}^{n+1} = \mathfrak{p}^n$ by Lemma 6. Define $\varphi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}^{n+1}$ by $\varphi(x) = \pi x \bmod \mathfrak{p}^{n+1}$. Then:

$$\begin{aligned} \operatorname{im}\varphi &= ((\pi) + \mathfrak{p}^{n+1})/\mathfrak{p}^{n+1} = \mathfrak{p}^n/\mathfrak{p}^{n+1}, \\ \ker\varphi &= \{x : \pi x \in \mathfrak{p}^{n+1}\} = \{x : \mathfrak{p}^{n+1} \mid (x)(\pi)\} = \{x : \mathfrak{p} \mid (x)\} = \mathfrak{p}. \end{aligned}$$ □

Corollary 14 *The norm is multiplicative:*

$$N(\mathfrak{a} \cdot \mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b}).$$

Proof. Use Theorem 12 and Lemma 13. □

Corollary 15 *For all ideals* $\mathfrak{a} \lhd \mathcal{O}_K$ *we have* $N(\mathfrak{a}) \in \mathfrak{a}$.

Proof. True for prime ideals as $\operatorname{char} \mathcal{O}_K/\mathfrak{p} \equiv 0 \mod \mathfrak{p}$ and hence lies in $\mathfrak{p}$. So true for all ideals by Cor. 14. Actually, it is obvious anyway: $N(\mathfrak{a})$ must be zero in any abelian group of order $N(\mathfrak{a})$. In particular $N(\mathfrak{a}) \equiv 0$ in $\mathcal{O}_K/\mathfrak{a}$. □

1.6. Enlarging the Field

14.10. **Example** Let $\mathbb{Q}(i)/\mathbb{Q}$. Take primes in $\mathbb{Q}$ and factorise them in $\mathbb{Q}(i)$:

$$\begin{array}{lcll} 2\mathbb{Z}[i] = (2) & = & (i+1)^2 & \text{“2 is ramified”}, \\ 3\mathbb{Z}[i] = (3) & & \text{remains prime} & \text{“3 is inert”}, \\ 5\mathbb{Z}[i] = (5) & = & (2+i)(2-i) & \text{“5 splits”}. \end{array}$$

Definition Let L/K be an extension of number fields and $\mathfrak{a} \lhd \mathcal{O}_K$ an ideal. The *conorm* of $\mathfrak{a}$ is the ideal $\mathfrak{a}\mathcal{O}_L$ of $\mathcal{O}_L$. Equivalently, if $\mathfrak{a} = (\alpha_1, \ldots, \alpha_n)$ as an $\mathcal{O}_K$-module then $\mathfrak{a}\mathcal{O}_L = (\alpha_1, \ldots, \alpha_n)$ as an $\mathcal{O}_L$-module.

Remark *(i)* $(\mathfrak{a}\mathcal{O}_L)(\mathfrak{b}\mathcal{O}_L) = (\mathfrak{a}\mathfrak{b})\mathcal{O}_L$.

(ii) $\mathfrak{a}\mathcal{O}_M = (\mathfrak{a}\mathcal{O}_L)\mathcal{O}_M$ when $K \subseteq L \subseteq M$.

Warning: Sometimes, we write $\mathfrak{a}$ for $\mathfrak{a}\mathcal{O}_L$ as well.

Proposition 16 *Let* L/K *be an extension of number fields and* $\mathfrak{a} \lhd \mathcal{O}_K$ *a non-zero ideal. Then:*

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

Proof. If $\mathfrak{a} = (\alpha)$ is principal, then by Lemma 9:

$$N(\mathfrak{a}\mathcal{O}_L) = |N_{L/\mathbb{Q}}(\alpha)| = |N_{K/\mathbb{Q}}(\alpha)|^{[L:K]} = N(\mathfrak{a})^{[L:K]},$$

so all is ok. In general, because $\mathcal{C}\ell_K$ is finite, $\mathfrak{a}^k = (\alpha)$ for some $k \geq 1$. Hence:

$$N(\mathfrak{a}\mathcal{O}_L)^k \overset{\text{C14}}{=} N(\mathfrak{a}^k\mathcal{O}_L) = N(\mathfrak{a}^k)^{[L:K]} \overset{\text{C14}}{=} N(\mathfrak{a})^{k[L:K]},$$

and so $N(\mathfrak{a}\mathcal{O}_L) = N(\mathfrak{a})^{[L:K]}$ as well. □

Definition A prime $\mathfrak{q}$ of L *lies above* a prime $\mathfrak{p}$ of K if $\mathfrak{q} \mid \mathfrak{p}\mathcal{O}_L$. (Equivalently if $\mathfrak{q} \supseteq \mathfrak{p}$.)

Lemma 17 *Let L/K be an extension of number fields. Every prime of L lies above a unique prime of K: $\mathfrak{q} \lhd \mathcal{O}_L$ lies above $(\mathfrak{q} \cap \mathcal{O}_K) \lhd \mathcal{O}_K$.*

Proof. First, $\mathfrak{q} \cap \mathcal{O}_K$ is a prime of $\mathcal{O}_L$, and it is non-zero since it contains e. g. $N(\mathfrak{q})$ (Cor. 15). So $\mathfrak{q}$ lies above $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$. If $\mathfrak{q}$ also lies above $\mathfrak{p}' \neq \mathfrak{p}$, then

$$\mathfrak{q} \supseteq \mathfrak{p} + \mathfrak{p}' = \mathcal{O}_K \ni 1,$$

which is a contradiction. □

Lemma 18 *Suppose $\mathfrak{q} \lhd \mathcal{O}_L$ lies above $\mathfrak{p} \lhd \mathcal{O}_K$. Then $\mathcal{O}_L/\mathfrak{q}$ is a field extension of $\mathcal{O}_K/\mathfrak{p}$.*

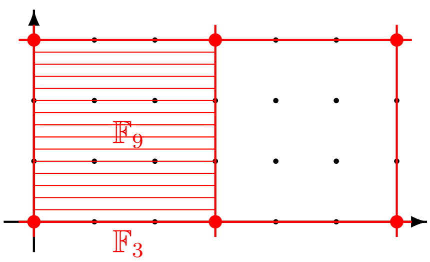
Proof. Define

$$\varphi : \mathcal{O}_K/\mathfrak{p} \longrightarrow \mathcal{O}_L/\mathfrak{q} \qquad \text{by} \qquad x \bmod \mathfrak{p} \longmapsto x \bmod \mathfrak{q}.$$

This is well defined as $\mathfrak{q}$ contains $\mathfrak{p}$. Moreover, φ is a ring homomorphism (with $1 \to 1$), so has no kernel as $\mathcal{O}_K/\mathfrak{p}$ is a field, i. e. it is an embedding $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{q}$. □

Remark (to the proof) The "reduction $\bmod\, \mathfrak{q}$" map on $\mathcal{O}_L$ extends the "reduction $\bmod\, \mathfrak{p}$" map on $\mathcal{O}_K$.

Example Let $\mathbb{Q}(i)/\mathbb{Q}$. Take $\mathfrak{p} = (3) \lhd \mathcal{O}_K$ and $\mathfrak{q} = (3) \lhd \mathcal{O}_L$:



Then $\mathbb{Z}/(3) \equiv \mathbb{F}_3$ sits inside $\mathbb{Z}[i]/(3) \equiv \mathbb{F}_9$ in the natural way. Note also that $(n) = n\mathbb{Z}[i]$ clearly has norm $n^2 = n^{[\mathbb{Q}(i):\mathbb{Q}]}$ (cf. Prop. 16).

Definition If $\mathfrak{q}$ lies above $\mathfrak{p}$, then its *residue degree* is $f_{\mathfrak{q}/\mathfrak{p}} = [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$. The *ramification degree* is the exponent $e_{\mathfrak{q}/\mathfrak{p}}$ in the prime factorisation $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}}$.

Theorem 19 *Let L/K be an extension of number fields and $\mathfrak{p}$ a prime of K.*

(i) *If $\mathfrak{p}\mathcal{O}_L$ decomposes as $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^m \mathfrak{q}_i^{e_i}$, with $\mathfrak{q}_i$ distinct and $e_i = e_{\mathfrak{q}_i/\mathfrak{p}}$, then:*

$$\sum_{i=1}^m e_{\mathfrak{q}_i/\mathfrak{p}} \cdot f_{\mathfrak{q}_i/\mathfrak{p}} = [L : K].$$

(ii) *If M/L is a further extension, $\mathfrak{r} \lhd \mathcal{O}_M$ lies above $\mathfrak{q} \lhd \mathcal{O}_L$ and $\mathfrak{q}$ lies above $\mathfrak{p} \lhd \mathcal{O}_K$, then:*

$$e_{\mathfrak{r}/\mathfrak{p}} = e_{\mathfrak{r}/\mathfrak{q}} \cdot e_{\mathfrak{q}/\mathfrak{p}} \qquad \textit{and} \qquad f_{\mathfrak{r}/\mathfrak{p}} = f_{\mathfrak{r}/\mathfrak{q}} \cdot f_{\mathfrak{q}/\mathfrak{p}}.$$

Proof. (i) Using Cor. 14 and Prop. 16:

$$\begin{aligned} N(\mathfrak{p})^{[L:K]} &= N(\mathfrak{p}\mathcal{O}_L) = N\left(\prod \mathfrak{q}_i^{e_i}\right) = \prod N(\mathfrak{q}_i)^{e_i} \\ &= \prod N(\mathfrak{p})^{f_{\mathfrak{q}_i/\mathfrak{p}} \cdot e_{\mathfrak{q}_i/\mathfrak{p}}} = N(\mathfrak{p})^{\sum f_{\mathfrak{q}_i/\mathfrak{p}} \cdot e_{\mathfrak{q}_i/\mathfrak{p}}}. \end{aligned}$$

(ii) Multiplicativity of e follows by writing out the prime decomposition of $\mathfrak{p}\mathcal{O}_M$. That of f is the tower law:

$$[\mathcal{O}_M/\mathfrak{r} : \mathcal{O}_L/\mathfrak{q}] \cdot [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}] = [\mathcal{O}_M/\mathfrak{r} : \mathcal{O}_K/\mathfrak{p}].$$ □

Definition Let L/K be an extension of number fields and $\mathfrak{p}$ a prime of K with $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^m \mathfrak{q}_i^{e_i}$. Then $\mathfrak{p}$ *splits completely* if $m = [L : K]$, i.e. $e_i = f_i = 1$ for all i; $\mathfrak{p}$ *splits* if $m > 1$; and $\mathfrak{p}$ is *totally ramified* in L if $m = f_i = 1$ and $e_i = [L : K]$. We will see that where L/K is Galois, then $e_i = e_j$ and $f_i = f_j$ for all i, j. Then we say that $\mathfrak{p}$ is *ramified* if $e_1 > 1$, and *unramified* if $e_1 = 1$.

Example (i) 5 splits (completely) in $\mathbb{Q}(i)/\mathbb{Q}$.

(ii) 2 is (totally) ramified in $\mathbb{Q}(i)/\mathbb{Q}$.

(iii) p is totally ramified in $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$.

16.10. **Theorem 20** (Kummer-Dedekind) *Let L/K be an extension of number fields. Suppose $\mathcal{O}_K[\alpha] \subseteq \mathcal{O}_L$ has finite index N for some $\alpha \in \mathcal{O}_L$ with minimal polynomial $f(x) \in \mathcal{O}_K[x]$. Let $\mathfrak{p} \lhd \mathcal{O}_K$ be a prime ideal not dividing N (so $\operatorname{char} \mathcal{O}_K/\mathfrak{p} \nmid N$). If*

$$f(x) \equiv \prod_{i=1}^m \bar{g}_i(x)^{e_i} \mod \mathfrak{p}$$

for distinct and irreducible g_i, then

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^m \mathfrak{q}_i^{e_i} \qquad \textit{with} \qquad \mathfrak{q}_i = \mathfrak{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L = (\mathfrak{p}, g_i(\alpha)),$$

where $g_i(x) \in \mathcal{O}_K[x]$ is such that $\bar{g}_i(x) \equiv g_i(x) \mod \mathfrak{p}$. The $\mathfrak{q}_i$ are distinct primes of L, with $e_{\mathfrak{q}_i/\mathfrak{p}} = e_i$ and $f_{\mathfrak{q}_i/\mathfrak{p}} = \deg \bar{g}_i(x)$.

Example Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_5)$ and $\mathcal{O}_L = \mathbb{Z}[\zeta_5]$. Take $\alpha = \zeta_5$, so $N = 1$ and $f(X) = X^4 + X^3 + X^2 + X + 1$. Then:

- $f(X) \bmod 2$ is irreducible, hence (2) is prime in $\mathcal{O}_L$.
- $f(X) \bmod 3$ is irreducible, hence (3) is prime in $\mathcal{O}_L$.
- $f(X) \bmod 5 = (X-1)^4$, hence $(5) = (5, \zeta_5 - 1)^4$.
- $f(X) \bmod 11 = (X-4)(X-9)(X-5)(X-3)$, hence $(11) = (11, \zeta - 4)(11, \zeta - 9)(11, \zeta - 5)(11, \zeta - 3)$.
- $f(X) \bmod 19 = (X^2+5X+1)(X^2-4X+1)$, hence $(19) = (19, \zeta^2+5\zeta+1)(19, \zeta^2 - 4\zeta + 1)$.

Example Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_{p^m})$ with p prime and $\mathcal{O}_L = \mathbb{Z}[\zeta_{p^m}]$. Then take $\alpha = \zeta_{p^m}$, so $N = 1$,

$$f(X) = \frac{X^{p^m} - 1}{X^{p^{m-1}} - 1}, \qquad f(X) \equiv (X-1)^{p^m - p^{m-1}} \mod p.$$

Thus p totally ramified in $\mathbb{Q}(\zeta_{p^m})$. If $p \neq q$ is also prime, then working $\bmod q$:

$$\gcd\left(X^{p^m} - 1, \frac{\mathrm{d}}{\mathrm{d}X}(X^{p^m} - 1)\right) = 1,$$

so $X^{p^m} - 1$ has no repeated roots in $\overline{\mathbb{F}}_q$, hence $f(X) \bmod q$ has no repeated roots, hence all e_i are 1, i. e. q is unramified in $\mathbb{Q}(\zeta_{p^m})$.

Remark We can't always find α, such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. However, by the Primitive Element Theorem, we can find α such that $L = K(\alpha)$. Scaling α if necessary gives $\alpha \in \mathcal{O}_L$ such that $L = K(\alpha)$; hence $\mathcal{O}_K$ has finite index in $\mathcal{O}_L$. So the theorem allows us to decompose all except possibly a finite number of primes.

Proof of Thm. 20. Write $A = \mathcal{O}_K[\alpha]$, $\mathbb{F} = \mathcal{O}_K/\mathfrak{p}$ and $p = \operatorname{char} \mathbb{F}$. Then we define

$$\mathcal{O}_K[X]/(f(X), \mathfrak{p}, g_i(X)) \xrightarrow{\sim} A/(\mathfrak{p}A + g_i(\alpha)A) \qquad \text{via} \qquad x \longmapsto \alpha, \qquad \text{with}$$
$$\mathcal{O}_K[X]/(f(X), \mathfrak{p}, g_i(X)) \cong \mathbb{F}[X]/(\bar{f}(X), \bar{g}_i(X)) \cong \mathbb{F}[X]/(\bar{g}_i(X)).$$

So this is a field of degree $f_i = \deg \bar{g}_i$ over $\mathbb{F}$, as $\bar{g}_i$ is irreducible.

Now pick $M \in \mathbb{Z}$ such that $NM \equiv 1 \mod p$ and consider

$$\varphi : A/(\mathfrak{p}A + g_i(\alpha)A) \longrightarrow \mathcal{O}_L/\mathfrak{q}_i, \qquad \varphi(x \bmod \mathfrak{p}A + g_i(\alpha)A) = x \bmod \mathfrak{q}_i.$$

This is well defined as $\mathfrak{q}_i \supseteq \mathfrak{p}A + g_i(\alpha)A$. Moreover, φ is surjective: If $x \in \mathcal{O}_L$ then $Nx \in A$, and

$$\varphi(MNx) \equiv MNx \equiv x \mod \mathfrak{q}_i$$

as $MN \equiv 1 \mod \mathfrak{q}_i$. We know that $\mathcal{O}_L/\mathfrak{q}_i$ is non-zero since otherwise $l \in \mathfrak{p}\mathcal{O}_L + g_i(X)\mathcal{O}_L$. So both p and NM are in $\mathfrak{p}A + g_i(\alpha)A$, hence $1 \in \mathfrak{p}A + g_i(\alpha)A$, which is a contradiction. Therefore $\mathcal{O}_L/\mathfrak{q}_i$ is a field extension of $\mathbb{F}$ of degree $f_i = \deg \bar{g}_i$ and $\mathfrak{q}_i$ is prime.

Now for $i \neq j$, as $\gcd(\bar{g}_i(x), \bar{g}_j(x)) = 1$, we can find $\lambda(X), \mu(X) \in \mathcal{O}_K[X]$ such that

$$\lambda(X)g_i(X) + \mu(X)g_j(X) \equiv 1 \mod \mathfrak{p}.$$

Then $\mathfrak{q}_i + \mathfrak{q}_j$ contains both $\mathfrak{p}$ and

$$\lambda(\alpha)g_i(\alpha) + \mu(\alpha)g_j(\alpha) \equiv 1 \mod \mathfrak{p},$$

so $\mathfrak{q}_i + \mathfrak{q}_j = \mathcal{O}_L$ and hence $\mathfrak{q}_i \neq \mathfrak{q}_j$ for $i \neq j$.

$$\prod_i \mathfrak{q}_i^{e_i} = \prod_i \left(\mathfrak{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L\right)^{e_i} \subseteq \mathfrak{p}\mathcal{O}_L + \left(\prod_i g_i(\alpha)^{e_i}\right)\mathcal{O}_L = \mathfrak{p}\mathcal{O}_L,$$

as $\prod g_i(\alpha)^{e_i} \equiv f(\alpha) \equiv 0 \mod \mathfrak{p}$. But

$$N\left(\prod \mathfrak{q}_i^{e_i}\right) = \prod \left(|\mathbb{F}|^{f_i}\right)^{e_i} = |\mathbb{F}|^{\deg f} = |\mathbb{F}|^{[L:K]} \overset{\text{P16}}{=} N(\mathfrak{p}\mathcal{O}_L),$$

so $\prod \mathfrak{q}_i^{e_i} = \mathfrak{p}\mathcal{O}_L$. □

Proposition 21 *Let $L/\mathbb{Q}$ be a finite extension, $\alpha \in \mathcal{O}_L$ with $L = \mathbb{Q}(\alpha)$ and minimal polynomial $f(X) \in \mathbb{Z}[X]$. If $f(X) \bmod p$ has distinct roots in $\overline{\mathbb{F}}_p$, then $\left[\mathcal{O}_L : \mathbb{Z}[\alpha]\right]$ is coprime to p. Hence, the Kummer-Dedekind Theorem applies.*

Proof. Let F be the splitting field of f with $f(X) = \prod(X - \alpha_i)$, $\alpha_i \in F$ and $\mathfrak{p}$ is a prime of F above p. As $f(X)$ has no repeated roots in $\overline{\mathbb{F}}_p$ and $\bar{f}(X) = \prod(X - \bar{\alpha}_i)$ (with $\bar{\alpha}_i$ denoting the reduction mod $\mathfrak{p}$), the $\bar{\alpha}_i$ are distinct in $\mathcal{O}_F/\mathfrak{p}$. Hence:

$$\prod_{i<j}(\alpha_i - \alpha_j) \not\equiv 0 \mod \mathfrak{p}.$$

Let $\beta_1, \ldots, \beta_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_L$, so $(1\ \alpha\ \ldots\ \alpha^{n-1})^\top = M(\beta_1\ \beta_2\ \ldots\ \beta_n)^\top$ for some $M \in \mathbb{Z}^{n\times n}$ with $\det M = \left[\mathcal{O}_L : \mathbb{Z}[\alpha]\right]$. Writing $\mathrm{id} = \sigma_1, \ldots, \sigma_n$ for the embeddings $L \hookrightarrow F$, we have

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

for some $B \in \mathcal{O}_F$. Hence $p \nmid \left[\mathcal{O}_L : \mathbb{Z}[\alpha]\right]$. □

Proposition 22 *Let K be a number field and $\mathfrak{p}$ a prime of K. Suppose $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathcal{O}_K[X]$ is Eisenstein with respect to $\mathfrak{p}$, i. e. $\mathfrak{p} \mid (a_i)$ for all i and $\mathfrak{p}^2 \nmid (a_0)$. Then, writing α for a root of f, $K(\alpha)/K$ has degree $n = \deg f$ and $\mathfrak{p}$ is totally ramified in $K(\alpha)$.*

Proof. See Local Fields (p. 48). □

2. Decomposition of Primes

2.1. Action of the Galois Group

Definition Let F/K be a finite Galois extension of number fields. By $\mathrm{Gal}(F/K) = \mathrm{Aut}_K(F)$ we denote the *Galois group* of F over K. Then: 19.10.

(*i*) F/K is normal, i. e. if $f \in K[x]$ is irreducible with a root in F then f has all its roots in F.

(*ii*) $|\,\mathrm{Gal}(F/K)| = [F : K]$.

(*iii*) We have a 1–1 correspondence between subgroups and intermediate fields:

$$\begin{array}{rcl} H \leq \mathrm{Gal}(F/K) & \longrightarrow & F^H, \\ \mathrm{Gal}(F/L) & \longleftarrow & K \subseteq L \subseteq F, \end{array}$$

where $F^H = \{x \in F : \sigma(x) = x \ \forall\, \sigma \in H\}$ denotes the fixed field of F under H. E. g.:

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_3, \sqrt[3]{2}) \arrow[dl, dash, "C_2"'] \arrow[dd, dash, "S_3"] \arrow[dr, dash, "C_3"] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash, "\text{not Galois}"'] & & \mathbb{Q}(\zeta_3) \arrow[dl, dash, "S_3/C_3 \cong C_2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Lemma 23 *Let* $g \in \mathrm{Gal}(F/K)$.

(*i*) *If* $\alpha \in \mathcal{O}_F$, *then* $g(\alpha) \in \mathcal{O}_F$, *i. e.* $\mathrm{Gal}(F/K)$ *acts on* $\mathcal{O}_F$.

(*ii*) *If* $\mathfrak{a} \lhd \mathcal{O}_F$ *is an ideal, then so is* $g(\mathfrak{a}) \lhd \mathcal{O}_F$.

(*iii*) *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are ideals, then:* $g(\mathfrak{a}\mathfrak{b}) = g(\mathfrak{a})g(\mathfrak{b})$ *and* $g(\mathfrak{a} + \mathfrak{b}) = g(\mathfrak{a}) + g(\mathfrak{b})$.

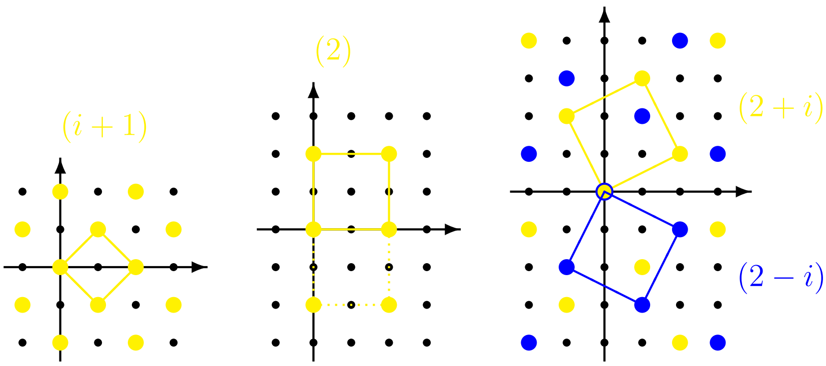
If $\mathfrak{q}$ *is a prime of* F *above* $\mathfrak{p}$, *a prime of* K, *then:*

(*iv*) $g(\mathfrak{q})$ *is a prime of* F *above* $\mathfrak{p}$, *i. e.* $\mathrm{Gal}(F/K)$ *permutes the primes above* F *over* $\mathfrak{p}$.

(*v*) $e_{\mathfrak{q}/\mathfrak{p}} = e_{g(\mathfrak{q})/\mathfrak{p}}$ *and* $f_{\mathfrak{q}/\mathfrak{p}} = f_{g(\mathfrak{q})/\mathfrak{p}}$.

Proof. Clear. □

Example Let $K = \mathbb{Q}$, $F = \mathbb{Q}(i)$, $\mathcal{O}_F = \mathbb{Z}[i]$ and $\mathrm{Gal}(F/K) = \{\mathrm{id}, \sigma\}$, where σ denotes the complex conjugation. Then:



- $(i+1)$ is fixed by $\mathrm{Gal}(F/K)$,
- (2) is fixed by $\mathrm{Gal}(F/K)$,
- $(2+i)$ and $(2-i)$ are swapped by $\mathrm{Gal}(F/K)$.

Theorem 24 *Let F/K be a Galois extension of number fields, $\mathfrak{p}$ a prime of K. Then $\mathrm{Gal}(F/K)$ acts transitively on the primes above $\mathfrak{p}$.*

Proof. Let $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ be the primes above $\mathfrak{p}$. Required to prove: There is a $g \in \mathrm{Gal}(F/K)$ such that $g(\mathfrak{q}_1) = \mathfrak{q}_2$. Then

$$\prod_{h \in \mathrm{Gal}(F/K)} h(x) \in \mathfrak{q}_1 \cap \mathcal{O}_K = \mathfrak{p} \subseteq \mathfrak{q}_2.$$

So for some $g \in \mathrm{Gal}(F/K)$ we have $g(x) \equiv 0 \mod \mathfrak{q}_2$. Thus $x \equiv 0 \mod g^{-1}(\mathfrak{q}_2)$, which implies $g^{-1}(\mathfrak{q}_2) = \mathfrak{q}_1$ and $g(\mathfrak{q}_1) = \mathfrak{q}_2$, respectively. □

Corollary 25 *Let F/K be a Galois extension of number fields. If $\mathfrak{q}_1$ and $\mathfrak{q}_2$ lie above $\mathfrak{p}$ then*

$$e_{\mathfrak{q}_1/\mathfrak{p}} = e_{\mathfrak{q}_2/\mathfrak{p}} \qquad \text{and} \qquad f_{\mathfrak{q}_1/\mathfrak{p}} = f_{\mathfrak{q}_2/\mathfrak{p}}.$$

So we can write $e_\mathfrak{p}$ and $f_\mathfrak{p}$.

Example Let F/K be a Galois extension of number fields and $\{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$ the set of primes above $\mathfrak{p}$. Knowing the action of Galois on $\{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$ allows us to easily find the number of primes above $\mathfrak{p}$ in any intermediate field L – it is the number of $\mathrm{Gal}(F/L)$-orbits on $\{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$. E. g. say $\mathrm{Gal}(F/K) \cong S_4$, and there are four primes $\mathfrak{q}_1, \dots, \mathfrak{q}_4$ in F above $\mathfrak{p}$, with S_4 acting in the usual way on the four points. Consider $H = \{\mathrm{id}, (1\ 2)(3\ 4)\} \leq S_4$ and $L = F^H$. Then $\mathrm{Gal}(F/L) = H$ acts transitively on the primes above every prime of L, so the number of primes above $\mathfrak{p}$ in L is equal to the number of H-orbits on $\{\mathfrak{q}_1, \dots, \mathfrak{q}_4\}$, which is 2.

2.2. The Decomposition Group

21.10. **Definition** Let F/K be a Galois extension of number fields, $\mathfrak{q}$ a prime of F above $\mathfrak{p}$, a prime of K. The *decomposition group* $D_{\mathfrak{q}}$ ($= \mathrm{D}_{\mathfrak{q}/\mathfrak{p}}$) of $\mathfrak{q}$ (over $\mathfrak{p}$) is the subgroup of $\mathrm{Gal}(F/K)$ fixing $\mathfrak{q}$, i. e.

$$D_{\mathfrak{q}/\mathfrak{p}} = \mathrm{Stab}_{\mathrm{Gal}(F/K)}(\mathfrak{q}) = \{g \in \mathrm{Gal}(F/K) : g(\mathfrak{q}) = \mathfrak{q}\}.$$

Remark Every $g \in D_{\mathfrak{q}}$ fixes $\mathfrak{q}$, so it acts on $\mathcal{O}_F/\mathfrak{q}$ by $x \bmod \mathfrak{q} \mapsto g(x) \bmod \mathfrak{q}$. This gives a natural map $D_{\mathfrak{q}} \to \mathrm{Gal}((\mathcal{O}_F/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p}))$.

Example Let $K = \mathbb{Q}$, $F = \mathbb{Q}(i)$ and $p = 3$. The complex conjugation acts as

$$a + bi \bmod 3 \longmapsto a - bi \bmod 3 = (a + bi)^3 \bmod 3,$$

i. e. exactly as the Frobenius automorphismus $x \mapsto x^3$ on $\mathbb{F}_9$.

Theorem 26 *Let F/K be a Galois extension of number fields, $\mathfrak{q}$ a prime of F above $\mathfrak{p}$, a prime of K. Then the natural map $D_{\mathfrak{q}} \to \mathrm{Gal}((\mathcal{O}_F/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p}))$ is surjective.*

Proof. Take $\beta \in \mathcal{O}_F/\mathfrak{q}$ with $\mathcal{O}_F/\mathfrak{q} = \mathcal{O}_K/\mathfrak{p}(\beta)$ (e. g. a generator for $(\mathcal{O}_K/\mathfrak{q})^\times$). Let $f(X) \in \mathcal{O}_K/\mathfrak{p}[X]$ be its minimal polynomial and $\beta = \beta_1, \dots, \beta_n \in \mathcal{O}_F/\mathfrak{q}$ its roots. (Note: As F/K is a Galois extension, all roots lie in $\mathcal{O}_F/\mathfrak{q}$.) Because $\mathrm{Gal}((\mathcal{O}_F/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p}))$ is cyclic, $g(\beta)$ determines $g \in \mathrm{Gal}((\mathcal{O}_F/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p}))$. So it suffices to prove that there is a $g \in \mathrm{Gal}(F/K)$ with $g(\mathfrak{q}) = \mathfrak{q}$ (i. e. $g \in D_{\mathfrak{q}/\mathfrak{p}}$) and $g(\beta) = \beta_2$. Pick $\alpha \in \mathcal{O}_F$ with $\alpha \equiv \beta \mod \mathfrak{q}$ and $\alpha \equiv 0 \mod \mathfrak{q}'$ for all other $\mathfrak{q}'$ above $\mathfrak{p}$. This is possible by the Chinese Remainder Theorem (Thm. 12). Let $F(X) \in \mathcal{O}_K[X]$ be its minimal polynomial over K and $\alpha = \alpha_1, \dots, \alpha_r \in \mathcal{O}_F$ its roots (again, all roots are in F since F/K is Galois). Then $F(X) \bmod \mathfrak{q}$ has β as a root, hence $F(X) \bmod \mathfrak{q}$ is divisible by $f(X)$, so $F(X) \bmod \mathfrak{q}$ has β_2 as a root. W. l. o. g. assume $\alpha_2 \equiv \beta_2 \mod \mathfrak{q}$. Now take $\mathrm{Gal}(F/K)$ with $g(\alpha) = \alpha_2$. Then $g(\alpha) \not\equiv 0 \mod \mathfrak{q}$, so $g(\mathfrak{q}) = \mathfrak{q}$ by choice of α, thus $g \in D_{\mathfrak{q}}$ and $g(\beta) = \beta_2$. □

Corollary 27 *Let K be a number field and F/K the splitting field of a monic irreducible polynomial $f(X) \in \mathcal{O}_K[X]$ of degree n. Let $\mathfrak{p}$ be a prime of K and*

$$f(X) \equiv g_1(X)g_2(X) \cdots g_k(X) \mod \mathfrak{p}$$

with $g_i(X) \in \mathcal{O}_K/\mathfrak{p}[X]$ distinct irreducible polynomials of degree $\deg g_i = d_i$. Then $\mathrm{Gal}(F/K) \subseteq S_n$ has an element of cycle type $(d_1, \dots, d_k)$.

Proof. Let $\mathfrak{q}$ be a prime above $\mathfrak{p}$. Let $\alpha_1, \dots, \alpha_n \in F$ be the roots of f. Note that $\alpha_i \bmod \mathfrak{q}$ is a root of $f \bmod \mathfrak{p}$ and that these are distinct (as the g_i are distinct). Thus the action of $g \in D_{\mathfrak{q}}$ on $\alpha_1, \dots, \alpha_n$ is exactly the same as on $\alpha_1 \bmod \mathfrak{q}, \dots \alpha_n \bmod \mathfrak{q}$. So take g which maps to the generator of $\mathrm{Gal}((\mathcal{O}_F/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p}))$ – it has the correct cycle type on the $\alpha_i \bmod \mathfrak{q}$. □

Definition Let F/K be a Galois extension of number fields and $\mathfrak{q}$ a prime above $\mathfrak{p}$. The *inertia subgroup* $I_{\mathfrak{q}} = I_{\mathfrak{q}/\mathfrak{p}}$ is the (normal) subgroup of $D_{\mathfrak{q}/\mathfrak{p}}$ that acts trivially on $\mathcal{O}_F/\mathfrak{q}$, i. e.:

$$I_{\mathfrak{q}} = \ker(D_{\mathfrak{q}} \longrightarrow \mathrm{Gal}((\mathcal{O}_F/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p}))).$$

Since $D_{\mathfrak{q}} \to \mathrm{Gal}((\mathcal{O}_F/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p}))$ is surjective, we have

$$D_{\mathfrak{q}}/I_{\mathfrak{q}} \cong \mathrm{Gal}((\mathcal{O}_F/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p})).$$

The latter is cyclic and generated by the Frobenius map $\varphi(x) = x^{|\mathcal{O}_K/\mathfrak{p}|}$. The (arithmetic) *Frobenius element* $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ is the element of $D_{\mathfrak{q}}/I_{\mathfrak{q}}$ that maps to φ.

Remark In Cor. 27, $I_{\mathfrak{q}/\mathfrak{p}}$ is trivial and $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ acts as the element of S_n of cyclic type $(d_1, \ldots, d_k)$.

Theorem 28 *Let F/K be a Galois extension of number fields and $\mathfrak{q}$ a prime of F above $\mathfrak{p}$, a prime of K. Then:*

(i) $|D_{\mathfrak{q}/\mathfrak{p}}| = e_{\mathfrak{q}/\mathfrak{p}} \cdot f_{\mathfrak{q}/\mathfrak{p}}$.

(ii) The order of $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ *is* $f_{\mathfrak{q}/\mathfrak{p}}$.

(iii) $|I_{\mathfrak{q}/\mathfrak{p}}| = e_{\mathfrak{q}/\mathfrak{p}}$.

If $K \subseteq L \subseteq F$ is an intermediate field and $\mathfrak{s}$ is a prime of L below $\mathfrak{q}$, then:

(iv) $D_{\mathfrak{q}/\mathfrak{s}} = D_{\mathfrak{q}/\mathfrak{p}} \cap \mathrm{Gal}(F/L)$.

(v) $I_{\mathfrak{q}/\mathfrak{s}} = I_{\mathfrak{q}/\mathfrak{p}} \cap \mathrm{Gal}(F/L)$.

Proof. (i) If n denotes the number of primes above $\mathfrak{p}$, then

$$n|D_{\mathfrak{q}/\mathfrak{p}}| = |\,\mathrm{Gal}(F/K)| = [F : K] = n \cdot e_{\mathfrak{q}/\mathfrak{p}} \cdot f_{\mathfrak{q}/\mathfrak{p}}.$$

(ii) We have

$$f_{\mathfrak{q}/\mathfrak{p}} = [\mathcal{O}_F/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}] = |\,\mathrm{Gal}((\mathcal{O}_F/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p}))|,$$

which is the order of $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$.

(iii) The order of the decomposition group $|D_{\mathfrak{q}/\mathfrak{p}}|$ is the order of the inertia group $|I_{\mathfrak{q}/\mathfrak{p}}|$ multiplyed by the order of the Frobenius element $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$, hence

$$|I_{\mathfrak{q}/\mathfrak{p}}| = \frac{e_{\mathfrak{q}/\mathfrak{p}} \cdot f_{\mathfrak{q}/\mathfrak{p}}}{f_{\mathfrak{q}/\mathfrak{p}}} = e_{\mathfrak{q}/\mathfrak{p}}.$$

The rest follows straight from the definition. □

23.10. **Example** Let $K = \mathbb{Q}$ and $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

(*i*) Let $p=2$, and $\mathfrak{q}$ be a prime in F above p. Then $(2)=(\sqrt{2})^2$ ramifies in $\mathbb{Q}(\sqrt{2})$. It also ramifies in $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$ since

$$X^2-3\equiv(X+1)^2 \mod 2, \qquad \text{and} \qquad X^2-6\equiv X^2 \mod 6.$$

This is enough to ensure that 2 is totally ramified in F: By the multiplicativity of e, we have $e_{\mathfrak{q}}\geq 2$, and so $|I_{\mathfrak{q}}|\geq 2$. Hence $I_{\mathfrak{q}}$ contains $\mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{d})\right)$ for one of $d=2,3,6$, so the prime above 2 ramifies in $F/\mathbb{Q}(\sqrt{d})$. Therefore $e_{\mathfrak{q}}=2\cdot 2=4$, and $I_{\mathfrak{q}}=C_2\times C_2$.

(*ii*) Let $p=3$, and $\mathfrak{q}$ be a prime in F above p. Then $(3)=(\sqrt{3})^2=(3,\sqrt{6})^2$ ramifies in $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$, but X^2-2 is irreducible modulo 3, and so (3) is prime in $\mathbb{Q}(\sqrt{2})$. Hence $e_3\geq 2$ and $f_3\geq 2$, so there is a unique prime above 3 in F, and $e_3=f_3=2$, i.e. (3) ramifies in $F/\mathbb{Q}(\sqrt{2})$. By $|D_{\mathfrak{q}}|=ef$, we obtain $I_{\mathfrak{q}}=\mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{2})\right)$, and $D_{\mathfrak{q}}=\mathrm{Gal}\left(F/\mathbb{Q}\right)$.

Example Let $K=\mathbb{Q}$ and $F=\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n^{th} root of unity. Let $p\nmid n$ be a prime, and $\mathfrak{q}$ a prime of F above p. We know that p is unramified, so $I_{\mathfrak{q}/p}=\{\mathrm{id}\}$ and $D_{\mathfrak{q}/p}=\langle\mathrm{Frob}_{\mathfrak{q}/p}\rangle$. The Frobenius element $\mathrm{Frob}_{\mathfrak{q}/p}$ acts as $x\mapsto x^p$ on $\mathcal{O}_F/\mathfrak{q}$, so $\mathrm{Frob}_{\mathfrak{q}/p}(\zeta_n)\equiv\zeta_n^p \mod \mathfrak{q}$. Since ζ_n^i are distinct in $\mathcal{O}_F/\mathfrak{q}$ as $X^n-1 \bmod p$ has distinct roots, this implies $\mathrm{Frob}_{\mathfrak{q}/p}(\zeta_n)=\zeta_n^p$. In particular, $f_{\mathfrak{q}/p}$ is the order of $\mathrm{Frob}_{\mathfrak{q}/p}$, and hence the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$.

2.3. Counting Primes

Lemma 29 *Let F/K be a Galois extension of number fields. Then:*

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

$$\mathfrak{p} \qquad \longleftrightarrow \qquad \textit{primes of } F \textit{ above } \mathfrak{p}.$$

(*ii*) *If $\mathfrak{q}$ is a prime of F above $\mathfrak{p}$ then $gD_{\mathfrak{q}}\mapsto g(\mathfrak{q})$ is a $\mathrm{Gal}(F/K)$-set isomorphism from $\mathrm{Gal}(F/K)/D_{\mathfrak{q}}$ to the set of primes above $\mathfrak{p}$.*

(*iii*) *The Galois group $\mathrm{Gal}(F/K)$ acts as conjugation on the decomposition group, the inertia group and the Frobenius element:*

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

Proof. Everything follows from transitivity of the action and elementary checks, respectively. □

Corollary 30 *Let F/K be a Galois extension of number fields and L an intermediate field. The there is a bijection between the set of primes of L above $\mathfrak{p}$, the $\mathrm{Gal}(F/L)$-orbits on primes of F above $\mathfrak{p}$ and the double cosets $H\backslash G/D_{\mathfrak{q}}$, where $H=\mathrm{Gal}(F/L)$, $G=\mathrm{Gal}(F/K)$ and $\mathfrak{q}$ is a prime of F above $\mathfrak{p}$ via the map that sends $\mathfrak{s}$ to the elements that send $\mathfrak{q}$ to some prime above $\mathfrak{s}$.*

Remark With $H\backslash G/D$ we mean the set $\{HgD : g \in G\}$, where $HgD = \{hgd : h \in H,\ d \in D\}$. These partition G but don't have equal size. The double cosets $H\backslash G/D$ correspond to the H-orbits on G/D and to the D-orbits on $H\backslash G$, where D acts by $d(Hg) = Hgd^{-1}$. What is the interpretation of D-orbits on $H\backslash G$? Let H be the stabiliser of α, where $L = K(\alpha)$, i. e. we want $D_{\mathfrak{q}}$-orbits on the roots of the minimal polynomials of α; equivalently on the embeddings $L \hookrightarrow F$.

Proposition 31 *Let F/K be a Galois extension of number fields, $L = K(\alpha)$ an intermediate field, $G = \mathrm{Gal}(F/K)$ and $H = \mathrm{Gal}(F/L)$. Let $\mathfrak{q}$ be a prime of F above $\mathfrak{s} \lhd \mathcal{O}_L$, and $\mathfrak{s}$ above $\mathfrak{p}$, a prime of K. Consider the G-set (of size $[L:K]$) $X = H\backslash G$ corresponding to the embeddings $L \hookrightarrow F$ and the roots of the minimal polynomial of α, respectively. Then there is a 1–1 correspondence between the primes of L above $\mathfrak{p}$ and the $D_{\mathfrak{q}}$-orbits on X, where $e_{\mathfrak{s}/\mathfrak{p}}f_{\mathfrak{s}/\mathfrak{p}}$ is the size of the $D_{\mathfrak{q}}$-orbit, $e_{\mathfrak{s}/\mathfrak{p}}$ is the size of any $I_{\mathfrak{q}}$-suborbit, and $f_{\mathfrak{s}/\mathfrak{p}}$ is the number of $I_{\mathfrak{q}}$-suborbits. Explicitly: $\mathfrak{s}$ maps to the orbit of $g^{-1}(\alpha)$, where $g(\alpha)$ lies above $\mathfrak{s}$.*

Proof. The 1–1 correspondence is the correspondence constructed in Cor. 30 and the last remark. Let N denote the size of the $D_{\mathfrak{q}}$-orbit of $g^{-1}(\alpha)$. Then:

$$\begin{aligned} N &= \frac{|D_{\mathfrak{q}}|}{|\operatorname{Stab}_{D_{\mathfrak{q}}}(g^{-1}(\alpha))|} = \frac{|D_{\mathfrak{q}}|}{|\operatorname{Stab}_{gD_{\mathfrak{q}}g^{-1}}(\alpha)|} \\ &= \frac{|D_{\mathfrak{q}}|}{|gD_{\mathfrak{q}}g^{-1} \cap H|} = \frac{|D_{\mathfrak{q}}|}{|D_{g(\mathfrak{q})}/\mathfrak{s}|} = \frac{e_{\mathfrak{q}/\mathfrak{p}}f_{\mathfrak{q}/\mathfrak{p}}}{e_{\mathfrak{q}/\mathfrak{s}}f_{\mathfrak{q}/\mathfrak{s}}}. \end{aligned}$$

Similarly, the size of $I_{\mathfrak{q}}$-orbits is $e_{\mathfrak{s}/\mathfrak{p}}$. (Note: This is independent of the subscript!) Moreover, the number of $I_{\mathfrak{q}}$-suborbits is

$$\frac{e_{\mathfrak{s}/\mathfrak{p}}f_{\mathfrak{s}/\mathfrak{p}}}{e_{\mathfrak{s}/\mathfrak{p}}} = f_{\mathfrak{s}/\mathfrak{p}}. \qquad \square$$

26.10. **Example** Let $K = \mathbb{Q}$, $F = \mathbb{Q}(\zeta_5, \sqrt[5]{2})$ and $p = 73$. Fix primes $\mathfrak{p}$ and $\mathfrak{q}$ above 73 in $\mathbb{Q}(\zeta_5)$ and F, respectively. First notice that 73 is a generator of $(\mathbb{Z}/5\mathbb{Z})^\times$, so $\mathfrak{p}$ has residue degree 4. Moreover, we know that $\mathfrak{q}/\mathfrak{p}$ is unramified since otherwise $5 \mid e_{\mathfrak{q}/73}$, which cannot happen as there is no ramification in $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$ by the Kummer-Dedekind Theorem (Thm. 20) because $X^5 - 2$ has distinct roots modulo 73. Hence we have $e_{\mathfrak{q}/73} = 1$ and $f_{\mathfrak{q}/73} = 4$ or $f_{\mathfrak{q}/73} = 20$, i. e. $I_{\mathfrak{q}} = \{\mathrm{id}\}$ and $D_{\mathfrak{q}} = C_4$ or $D_{\mathfrak{q}} = C_{20}$ (generated by $\mathrm{Frob}_{\mathfrak{q}/73}$). But C_{20} is not a subgroup of $\mathrm{Gal}(F/\mathbb{Q}) \leq S_5$, and so $D_{\mathfrak{q}} = C_4$. Now take $L = \mathbb{Q}(\sqrt[5]{2})$. Then $\mathrm{Gal}(F/\mathbb{Q})$ permutes $\sqrt[5]{2}, \zeta_5\sqrt[5]{2}, \ldots, \zeta_5^4\sqrt[5]{2}$. W. l. o. g. we can assume that $D_{\mathfrak{q}}$ fixes $\sqrt[5]{2}$, and permutes the others cyclicly, while $I_{\mathfrak{q}}$ fixes all five. Hence there are two primes in L above 73, with residue degrees 1 and 4, and ramification degrees 1 and 1, respectively.

Example (Euler's Criterion ++) Recall: a is a square modulo p iff $a^{\frac{p-1}{2}} \equiv 1 \mod p$, for $p \nmid n$. This follows from the cyclicity of $\mathbb{F}_p^\times$. Similar, for $p \nmid 3a$:

- $X^3 - a$ has three roots modulo p iff $a^{\frac{p-1}{3}} \equiv 1 \mod p$.
- $X^3 - a$ is irreducible modulo p iff $a^{\frac{p-1}{3}}$ is a root of $X^2 + X + 1$ modulo p.

- $X^3 - a$ has one root modulo p iff $p \equiv 2 \mod 3$.

For a generic polynomial, we cannot exploit the cyclicity of $\mathbb{F}_p^\times$. Instead: Let $f(X) = X^3 + bX + c$, with $b, c \in \mathbb{Z}$, and F be its splitting field, with roots α, β, and γ. For $g \in S_3$ (permuting α, β, and γ) consider

$$\alpha g(\alpha) + \beta g(\beta) + \gamma g(\gamma).$$

It is a root of one of

$$\begin{aligned}
\Gamma_1 &= X - (\alpha^2 + \beta^2 + \gamma^2) = X - (\alpha + \beta + \gamma)^2 + 2(\alpha\beta + \alpha\gamma + \beta\gamma) = X + 2b, \\
\Gamma_2 &= \left(X - (\alpha\beta + \beta\alpha + \gamma^2)\right)\left(X - (\alpha\gamma + \beta^2 + \gamma\alpha)\right)\left(X - (\alpha^2 + \beta\gamma + \gamma\beta)\right) \\
&= X^3 - 3b^2 X - b^3 - 27c^2, \\
\Gamma_3 &= (X - (\alpha\beta + \beta\gamma + \gamma\alpha))(X - (\alpha\gamma + \beta\alpha + \gamma\beta)) = (X - b)^2.
\end{aligned}$$

(Simply oben brackets, and rewrite in terms of the symmetric functions $\alpha + \beta + \gamma = 0$, $\alpha\beta + \alpha\gamma + \beta\gamma = b$, and $\alpha\beta\gamma = -c$.) Now take p, and a prime $\mathfrak{q}$ above p in F. To determine the factorisation of $f(X)$ modulo p, look at $\mathrm{Frob}_{\mathfrak{q}/p}$: If $f(X)$ has distinct roots modulo p (this is equivalent to $p \nmid 4b^3 + 27c^2$) then the number of roots modulo p is equal to the number of fixed points of $\mathrm{Frob}_{\mathfrak{q}/p}$. (The action of $\mathrm{Frob}_{\mathfrak{q}/p}$ on α, β, and γ corresponds to the action of $\varphi : x \mapsto x^p$ on α, β, and γ modulo $\mathfrak{q}$.) So compute

$$\begin{aligned}
\alpha \,\mathrm{Frob}_{\mathfrak{q}/p}(\alpha) + \beta \,\mathrm{Frob}_{\mathfrak{q}/p}(\beta) + \gamma \,\mathrm{Frob}_{\mathfrak{q}/p}(\gamma) &\equiv \alpha^{p+1} + \beta^{p+1} + \gamma^{p+1} \mod \mathfrak{q} \\
&\equiv \mathrm{Tr} \begin{bmatrix} 0 & 0 & -c \\ 1 & 0 & -b \\ 0 & 1 & 0 \end{bmatrix}^{p+1} \mod p \\
&\left(= \mathrm{Tr}_{\mathbb{F}_p[X]/(X^2+bX+c)}(x^{p+1})\right),
\end{aligned}$$

where we could have taken any matrix with eigenvalues α, β, and γ. Therefore, if $p \nmid 3b(4b^2 + 27c^2)$ (so Γ_1, Γ_2, and Γ_3 have no common roots modulo p) then $f(X)$ has three roots modulo p. Let T denote the trace of the above matrix, then this is equivalent to $T \equiv -2b \mod p$. Furthermore, $f(X)$ is irreducible iff $T \equiv b \mod p$, and $f(X)$ has one root iff T is a root of $X^3 - 3b^2X - 2b^3 - 27c^3$ modulo p.

2.4. Interlude: Induced Representations

Definition Let G be a finite group. If X is a finite G-set (of size n), we associate to it the n-dimensional *representation* $\mathbb{C}[X]$ which has $\{e_x\}_{x \in X}$ as a basis and with G-action

$$g\left(\sum \lambda_x e_x\right) = \sum \lambda_x e_{g(x)}.$$

The number of G-orbits on X can be recovered as $\langle \mathbf{1}, \mathbb{C}[X] \rangle$. The *character* of $\mathbb{C}[X]$ is given by

$$\chi_{\mathbb{C}[X]}(g) = \#\{x \in X : g(x) = x\}.$$

Let H be a subgroup of G of index n and let V be an H-representation. The *induction* of V to G is

$$\mathrm{Ind}_H^G V := \mathrm{Hom}_{\mathbb{C}[G], V}.$$

Concretely, if $g_1, \dots, g_n$ is a set of left coset representatives of H, take $\operatorname{Ind} V$ to be n copies of V with G-action determined by

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

where the i^{th} entry v gives the j^{th} entry $h(v)$ when $gg_i = g_j h$ with $h \in H$. Note that if $V = \mathbf{1}$ then $\operatorname{Ind}_H^G V$ simply gives $\mathbb{C}[G/H]$. The *character formula* is

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

We have: $\dim \operatorname{Ind}_H^G \varrho = [G : H] \cdot \dim \varrho$.

Example (Induction vs Restriction) Take $G = S_4$ and $H = S_3 \leq G$. The character tables are:

	1	$(**)$	$(***)$	$(**)(**)$	$(****)$
$\mathbf{1}$	1	1	1	1	1
s	1	-1	1	1	-1
T	2	0	-1	2	0
V	3	1	0	-1	-1
W	3	-1	0	-1	1

	1	$(**)$	$(***)$
$\mathbf{1}$	1	1	1
ε	1	-1	1
ϱ	2	0	-1

Representations restrict from G to H as follows (trivial computation):

- $\operatorname{Res}_H^G \mathbf{1} = \mathbf{1}$,
- $\operatorname{Res}_H^G s = \varepsilon$,
- $\operatorname{Res}_H^G T = \varrho$,
- $\operatorname{Res}_H^G V = \mathbf{1} \oplus \varrho$, and
- $\operatorname{Res}_H^G W = \varepsilon \oplus \varrho$.

Induction from H to G works as:

- $\operatorname{Ind}_H^G \mathbf{1} = \mathbf{1} \oplus V$,
- $\operatorname{Ind}_H^G \varepsilon = s \oplus W$, and
- $\operatorname{Ind}_H^G \varrho = T \oplus V \oplus W$.

Theorem (Frobenius Reciprocity) *For V a representation of H and W a representation of G with $H \leq G$ we have*

$$\left\langle V, \operatorname{Res}_H^G W \right\rangle_H = \left\langle \operatorname{Ind}_H^G V, W \right\rangle_G.$$

Theorem (Mackey's Formula) *Let $D, H \leq G$ and let ϱ be an H-representation. Fix $X = \{x_1, \dots, x_n\}$ a set of H–D double coset representatives, and for $x \in X$ define the $x^{-1}Hx$-representation ϱ^x by $\varrho^x(x^{-1}gx) = \varrho(g)$. Then:*

$$\operatorname{Res}_D^G \operatorname{Ind}_H^G \varrho \cong \bigoplus_{x \in X} \operatorname{Ind}_{x^{-1}Hx \cap D}^D \operatorname{Res}_{x^{-1}Hx \cap D}^{x^{-1}Hx} \varrho^x.$$

2.5. Representations of the Decomposition Group

Fix the following setting: Let F/K be a Galois extension of number fields, $\mathfrak{p}$ a prime of K, $\mathfrak{q}$ lies above $\mathfrak{p}$, $D = D_{\mathfrak{q}/\mathfrak{p}}$, $I = I_{\mathfrak{q}/\mathfrak{p}}$, $\mathrm{Frob} = \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$, and $G = \mathrm{Gal}(F/K)$. 28.10.

Remark If L is an intermediate field and $H = \mathrm{Gal}(F/L)$. Then the number of primes of L above $\mathfrak{p}$ is equal to the number of H-orbits on G/D (Cor. 30), which is equal to $\left\langle \mathrm{Res}_H^G \mathrm{Ind}_D^G \mathbf{1}_D, \mathbf{1}_H \right\rangle_H = \left\langle \mathbf{1}_D, \mathrm{Res}_D^G \mathrm{Ind}_H^G \mathbf{1}_G \right\rangle_D$, which is the number of D-orbits on the embeddings $G \hookrightarrow F$ as in Prop. 31.

Definition If V is a representation of D, write V^I for the subspace of I-invariant vectors. As $I \lhd D$, this is a subrepresentation.

Exercise Check this – if $v \in V^I$ then so is gv, because for $h \in I$, we have $h(gv) = gh'v = gv$ for some $h' \in I$.

Lemma 32 *If V is an irreducible representation of D, then either $V^I = 0$ or V is 1-dimensional, lifted from $D/I = \langle \mathrm{Frob} \rangle$, i. e. $D \to D/I \to \mathbb{C}^\times$. (These kill I and are determined by the action of* Frob.*)*

Proof. As V^I is a subrepresentation, we have $V^I = 0$ or $V^I = V$. If $V^I = V$, then the action of D factors through D/I. The latter is abelian, so V is 1-dimensional. $\square$

Remark So representations of D look like $V = A \oplus B$ with $A^I = 0$ and $B^I = V^I$, which is the direct sum of 1-dimensional representations of D/I. (A representation with $V^I = V$ is called *unramified*, else *ramified*.)

Definition For the characteristic polynomial of the Frobenius element on V^I we write

$$\Phi_{\mathfrak{q}/\mathfrak{p}}(V, t) := \det_{V^I}(t\,\mathrm{id} - \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}).$$

Lemma 33 *Let $\psi : D \to D/I \to \mathbb{C}^\times$ be a 1-dimensional representation of D with $\psi(\mathrm{Frob}) = \zeta$, a root of unity. Then $\langle \psi, V \rangle = \left\langle \psi, V^I \right\rangle$ is equal to the multiplicity of $(t - \zeta)$ in $\Phi_{\mathfrak{q}/\mathfrak{p}}(V, t)$.*

Proof. Clear from the previous remark. $\square$

Remark Thus Φ simply encodes the multiplicities of the 1-dimensional representation of D/I in representation of D.

Proposition 34 *Let $K \subseteq L \subseteq F$ be an intermediate field and V a representation of $H = \mathrm{Gal}(F/L)$. Then*

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

where $\mathfrak{s}$ ranks over the primes of L above $\mathfrak{p}$, and $\mathfrak{q}$, a prime of F, lies above $\mathfrak{s}$.

Proof. We will show that the LHS and the RHS have the same roots, with the same multiplicities. Note that the roots are $f_{\mathfrak{q}/\mathfrak{p}}{}^{\text{th}}$ roots of unity. Let ζ be such a root and take $\psi : D \to D/I \to \mathbb{C}^\times$ with $\psi(\text{Frob}) = \zeta$. Let N denote the multiplicity of $t - \zeta$ in LHS, then:

$$\begin{aligned}
N &\overset{\text{L33}}{=} \left\langle \psi, \operatorname{Res}_D \operatorname{Ind}_H^G V \right\rangle_D \\
&\overset{\text{Mackey}}{=} \sum_{x \in H\backslash G/D} \left\langle \psi, \operatorname{Ind}^D_{x^{-1}Hx\cap D} \operatorname{Res}^{x^{-1}Hx}_{x^{-1}Hx\cap D} V^x \right\rangle_D \\
&\overset{\text{L29(i)}}{=} \sum_{\mathfrak{s}} \left\langle \psi^{x^{-1}}, \operatorname{Ind}^{D_{\mathfrak{q}_i/\mathfrak{p}}}_{D_{\mathfrak{q}_i/\mathfrak{s}}} \operatorname{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V \right\rangle_{D_{\mathfrak{q}_i/\mathfrak{p}}} \\
&\overset{\text{Frob. Rec.}}{=} \sum_{\mathfrak{s}} \left\langle \operatorname{Res}^{D_{\mathfrak{q}_i/\mathfrak{p}}}_{D_{\mathfrak{q}_i/\mathfrak{s}}} \psi^{x^{-1}}, \operatorname{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V \right\rangle_{D_{\mathfrak{q}_i/\mathfrak{p}}} \\
&\overset{\text{L33}}{=} \sum_{\mathfrak{s}} \text{ mult. of } t - \zeta^{f_{\mathfrak{s}/\mathfrak{p}}} \text{ in } \Phi_{\mathfrak{q}_i/\mathfrak{s}}(\operatorname{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V, t) \\
&= \sum_{\mathfrak{s}} \text{ mult. of } t - \zeta \text{ in } \Phi_{\mathfrak{q}_i/\mathfrak{s}}(\operatorname{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V, t^{f_{\mathfrak{s}/\mathfrak{p}}}).
\end{aligned}$$

□

Corollary 35 *Take $\psi_n : D \to D/I \to \mathbb{C}^\times$ which maps* Frob *to a primitive n^{th} root of unity (with $n \mid f_{\mathfrak{q}/\mathfrak{p}}$). Then the number of primes $\mathfrak{s}$ of L above $\mathfrak{p}$ with $n \mid f_{\mathfrak{s}/\mathfrak{p}}$ is equal to $\left\langle \psi_n, \operatorname{Res}^G_D \operatorname{Ind}^G_H \mathbf{1}_H \right\rangle_D$.*

Proof. We have:

$$\begin{aligned}
\left\langle \psi_n, \operatorname{Res}^G_D \operatorname{Ind}^G_H \mathbf{1}_H \right\rangle_D &\overset{\text{L33}}{=} \text{mult. of } t - \zeta_n \text{ in } \Phi_{\mathfrak{q}/\mathfrak{p}}(\operatorname{Res}_D \operatorname{Ind}^G \mathbf{1}, t) \\
&\overset{\text{P34}}{=} \text{mult. of } t - \zeta_n \text{ in } \prod_{\mathfrak{s}} \Phi_{\mathfrak{q}_i/\mathfrak{p}}(\mathbf{1}, t^{f_{\mathfrak{s}/\mathfrak{p}}}) \\
&= \text{mult. of } t - \zeta_n \text{ in } \prod_{\mathfrak{s}} (t^{f_{\mathfrak{s}/\mathfrak{p}}} - 1) \\
&= \text{number of primes } \mathfrak{s} \text{ with } n \mid f_{\mathfrak{s}/\mathfrak{p}}.
\end{aligned}$$

□

Exercise Deduce Cor. 35 straight from Prop. 31.

3. L-Series

In this chapter, we want to prove two statements: 30.10.

(*i*) If $(a, n) = 1$ then there are infinitely many primes $p \equiv a \mod n$.

(*ii*) If $f(X) \in \mathbb{Z}[X]$ monic and $f(X) \bmod p$ has a root for every prime p, then f is reducible.

The method will use certain infinite series.

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

$$f(s) = \sum_{n=1}^{\infty} a_n n^{-s}, \qquad a_n \in \mathbb{C}, \quad s \in \mathbb{C}.$$

Warning: Traditionally, the complex variable is $s = \sigma + it$.

3.1. Convergence Properties

Lemma 36 (Abel's Lemma) *Let a_n and b_n be sequences in $\mathbb{C}$. Then:*

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

Proof. Elementary rearrangement. Cf. integration by parts with $a \leftrightarrow \mathrm{d}v$ and $b \leftrightarrow \mathrm{d}u$:

$$\int u \, \mathrm{d}v = [uv] - \int v \, \mathrm{d}u. \qquad \square$$

Proposition 37 *Let $f(s) = \sum a_n \mathrm{e}^{-\lambda_n s}$ where $\lambda_n \to \infty$ is an increasing sequence of positive real numbers.*

(i) If the partial sums $\sum_{n=N}^{M} a_n$ are bounded, then the series converges locally uniformly on $\Re(s) > 0$ to an analytic function.

(ii) If the series $f(s)$ converges for $s = s_0$, then it converges locally uniformly on $\Re(s) > \Re(s_0)$ to an analytic function.

Note: Dirichlet series are a special case for $\lambda_n = \log n$.

Proof. First note that the first statement implies the second one. Change the variables: $s' = s - s_0$ and $a'_n = \mathrm{e}^{-\lambda_n - s_0} a_n$. The new series converges at 0 and so must have $\sum_{n=N}^{M} a'_n$ bounded. Then invoke (i).

Now we will show uniform convergence on $-A < \operatorname{Arg}(s) < A$, with $\Re(s) > \delta$. This will suffice, as the uniform limit of analytic functions is analytic. Let $\varepsilon > 0$. Find N_0 such that for $n > N_0$ we have $|\mathrm{e}^{-\lambda_n s}| < \varepsilon$ in this domain. Now compute for $N, M \geq N_0$:

$$\begin{aligned}\left|\sum_{n=N}^{M} a_n \mathrm{e}^{-\lambda_n s}\right| &\overset{\text{L36}}{=} \left|\sum_{n=N}^{M-1}\left(\sum_{k=N}^{n} a_k\right)\left(\mathrm{e}^{-\lambda_n s} - \mathrm{e}^{-\lambda_{n+1} s}\right) + \left(\sum_{k=N}^{M} a_k\right)\mathrm{e}^{-\lambda_n s}\right| \\ &\leq B \cdot \sum_{n=N}^{M-1}\left|\left(\mathrm{e}^{-\lambda_n s} - \mathrm{e}^{-\lambda_{n+1} s}\right)\right| + B\varepsilon,\end{aligned}$$

where B is the bound on $|\sum a_k|$. Observe:

$$\left|\mathrm{e}^{-\alpha s} - \mathrm{e}^{-\beta s}\right| = \left|s\int_\alpha^\beta \mathrm{e}^{-xs}\,\mathrm{d}x\right| \leq |s| \cdot \int_\alpha^\beta \left|\mathrm{e}^{-x\sigma}\right|\mathrm{d}x = \frac{|s|}{\sigma}\left(\mathrm{e}^{-\alpha\sigma} - \mathrm{e}^{-\beta\sigma}\right),$$

where $\sigma = \Re(s)$. So we have:

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

where $\frac{|s|}{\sigma} \leq K$ in our domain. Hence we have uniform convergence. □

Proposition 38 *Let $f(s) = \sum a_n \mathrm{e}^{-\lambda_n s}$ where $\lambda_n \to \infty$ is an increasing sequence of positive real numbers. Suppose that $a_n \in \mathbb{R}_{\geq 0}$, the series $f(s)$ converges on $\Re(s) > R$ for some $R \in \mathbb{R}$ (and is hence analytic there), and it has an analytic continuation to a neighbourhood of $s = R$. Then $f(s)$ converges on $\Re(s) > R - \varepsilon$ for some $\varepsilon > 0$.*

Proof. Again we may assume $R = 0$. Since f is analytic on $\Re(s) > 0$ and on $|s| < \delta$, f is analytic on $|s - 1| \leq 1 + \varepsilon$. The Taylor series of f around $s = 1$ converges on all of $|s - 1| \leq 1 + \varepsilon$, in particular

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

converges. For $\Re(s) > 0$, we have

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

The term-by-term derivation is allowed by the locally uniform convergence. Thus we have

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

a convergent series with positive terms. Hence:

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

Note that the order of summation does not matter as all terms are positive. This is a convergent series, thus the series for f converges at $s = -\varepsilon$ and hence on $\Re(s) > -\varepsilon$ by Prop. 37. □

Theorem 39 *(i) If a_n are bounded, then $\sum a_n n^{-s}$ converges absolutely on $\Re(s) > 1$ to an analytic function.*

(ii) If the partial sums $\sum_{n=N}^{M} a_n$ are bounded, then $\sum a_n n^{-s}$ converges on $\Re(s) > 0$ to an analytic function.

Proof. (i) Since $\sum n^{-x}$ converges for real $x > 1$, analyticity follows from Prop. 37:

$$\left|\sum \frac{a_n}{n^s}\right| \le \sum \frac{|a_n|}{n^\sigma} \le K \cdot \sum \frac{1}{n^x} \qquad \text{for } x > 1.$$

(ii) Follows immediately from Prop. 37.

□

Exercise If $\sum a_n \mathrm{e}^{-\lambda_n s}$ and $\sum b_n \mathrm{e}^{-\lambda_n s}$ converge on $\Re(s) > \sigma_0$ to the same function $f(s)$, then $a_n = b_n$ for all n.

3.2. Dirichlet L-Functions

Definition Let $N \ge 1$ be an integer and $\psi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ a group homomorphism. 02.11
Extend ψ to a function on $\mathbb{Z}$ by

$$\psi(n) = \begin{cases} \psi(n \bmod N), & \text{if } (n, N) = 1, \\ 0, & \text{else.} \end{cases}$$

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 The map $\psi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is also sometimes referred to as a Dirichlet character. *Warning*: Note that $\psi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is simply a 1-dimensional representation. Number theorists have the (bad) habit of referring to 1-dimensional representations as characters.

Lemma 40 *Let ψ be a Dirichlet character modulo N. Then:*

(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 satisfies the Euler product:

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

Proof. The first two statements are obvious from the definition. The L-series coefficients $\psi(n)$ are bounded, so absolute convergence follows from Thm. 39 (i). For $\Re(s) > 1$ we have:

$$\sum \psi(n)n^{-s} = \prod_{p\in\mathbb{P}} \left(1 + \psi(p)p^{-s} + \psi(p)^2p^{-2s} + \ldots\right) = \prod_{p\in\mathbb{P}} \frac{1}{1-\psi(p)p^{-s}},$$

by (ii), the absolute convergence and the geometric series. □

Example Take $N = 10$, so $(\mathbb{Z}/N\mathbb{Z})^\times = \{1, 3, 5, 7\} \cong C_4$ and take $\psi(1) = 1$, $\psi(3) = i$, $\psi(7) = -i$ and $\psi(9) = -1$. Then:

$$L_{10}(\psi, s) = 1 + \frac{i}{3^s} - \frac{i}{7^s} - \frac{1}{9^s} + \frac{1}{11^s} + \frac{i}{13^s} - \frac{i}{15^s} - \frac{1}{19^s} \pm \ldots$$

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

$$L_N(\mathbf{1}, s) = \zeta(s) \cdot \prod_{p|N}(1 - p^{-s}),$$

where $\zeta(s) = \sum n^{-s}$ is the *Riemann ζ-function*.

Theorem 41 *Let $N \geq 1$ and $\psi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$.*

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

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

Proof. (*i*) Follows from the last remark and the fact that $\zeta(s)$ has an analytic continuation to $\Re(s) > 0$, except for a simple pole at $s = 1$.

(*ii*) We have a representation of $(\mathbb{Z}/N\mathbb{Z})^\times$ and ψ is non-trivial, so

$$\sum_{n=A}^{A+N-1} \psi(n) = \sum_{n\in(\mathbb{Z}/N\mathbb{Z})^\times} \psi(n) = \langle \psi, \mathbf{1} \rangle = 0.$$

So the sums $\sum_{n=A}^{B} \psi(n)$ are bounded, and the result follows from Thm. 39 (ii). □

Theorem 42 *Let ψ be a non-trivial Dirichlet character modulo N. Then the L-function does not vanish at $s = 1$, i. e. $L_N(\psi, 1) \neq 0$.*

Proof. Let

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

Suppose $L_N(\psi, s) = 0$. Then $\zeta_N(s)$ has an analytic continuation to $\Re(s) > 0$ by Thm. 41, the pole from $L_N(\mathbf{1}, s)$ having been killed by the zero of $L_N(\psi, s)$. On $\Re(s) > 1$, $\zeta_N(s)$ has the absolute convergent Euler product

$$\zeta_N(s) = \prod_\chi \prod_p \frac{1}{1 - \chi(p)p^{-s}} = \prod_{p \nmid N} \prod_\chi \frac{1}{1 - \chi(p)p^{-s}}.$$

Now

$$\prod_\chi (1 - \chi(p)T) = (1 - T^{f_p})^{\varphi(N)/f_p},$$

where f_p is the order of $p \bmod N$ and φ is the Euler totient function. Indeed the $\chi(p)$ are ${f_p}^{\text{th}}$ roots of unity, each occuring $\varphi(N)/f_p$ times, and

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

So on $\Re(s) > 1$, $\zeta_N(s)$ is a Dirichlet series given by

$$\zeta_N(s) = \prod_{p \nmid N} \left(1 + p^{-f_p s} + p^{-2 f_p s} + \ldots\right)^{\varphi(N)/f_p}.$$

By Prop. 38, as $\zeta_N(s)$ is assumed analytic on $\Re(s) > 0$ and this series has positive coefficients, the series must converge on $\Re(s) > 0$. But for $s \geq 0$ real it dominates

$$\prod_{p \nmid N} \left(1 + p^{-\varphi(N)s} + p^{-2\varphi(N)s} + \ldots\right) = L_N(\mathbf{1}, \varphi(N)s),$$

which diverges for $s = 1/\varphi(N)$. So we have a contradiction. □

3.3. Primes in Arithmetic Progressions

Proposition 43 *Let ψ be a Dirichlet character modulo N.* 04.11.

(i) The Dirichlet series

$$\sum_{p \in \mathbb{P}, n \geq 1} \frac{\psi(p)^n}{n} p^{-ns}$$

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 non-trivial then $\sum \frac{\psi(p)^n}{n} p^{-ns}$ is bounded as $s \to 1$. If $\psi = \mathbf{1}$ then for $s \to 1$:

$$\sum_{p \in \mathbb{P}, n \geq 1} \frac{\psi(p)^n}{n} p^{-ns} \sim \log \frac{1}{s-1}.$$

Proof. (*i*) The series has bounded coefficients, so converges absolutely on $\Re(s) > 1$ to an analytic function by Thm. 39 (i). For fixed s with $\Re(s) > 1$, we have

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

Hence $\sum \frac{\psi(p)^n}{n} p^{-ns}$ is an analytic branch of $\log L_N(\psi, s)$ on $\Re(s) > 1$.

(*ii*) By Thm. 41, if ψ is non-trivial, then $L_N(\psi, s)$ converges to a non-zero value as $s \to 1$, so its logarithm is bounded near $s = 1$. For the trivial character, $L_N(\mathbf{1}, s)$ has a simple pole at $s = 1$ (hence $\sim \frac{\lambda}{s-1}$), so for $s \to 1$:

$$\log L_N(\psi, s) \sim \log \frac{1}{s-1}.$$

□

Corollary 44 *(i) If ψ is non-trivial, then $\sum \psi(p) p^{-s}$ is bounded as $s \to 1$.*

(ii) If $\psi = \mathbf{1}$ then

$$\sum_p \psi(p) p^{-s} = \sum_{p \nmid N} p^{-s} \sim \log \frac{1}{s-1}$$

as $s \to 1$. In particular it diverges to infinity as $s \to 1$.

Remark The second statement implies that there are infinitely many primes.

Proof. We have

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

so it is sufficient to check that the last term is bounded on $\Re(s) > 1$. But if $\Re(s) > 1$ then

$$\left| \sum_{p, n \geq 2} \frac{\psi(p)^n}{n} p^{-ns} \right| \leq \sum_{p, n \geq 2} \frac{1}{|p^s|^n} = \sum_p \frac{1}{|p^s|(|p^2| - 1)} \leq \sum_p \frac{1}{p(p-1)} \leq \sum_{k=1}^{\infty} \frac{1}{k^2} < \infty,$$

as $\Re(s) > 1$. □

Theorem 45 (Dirichlet's Theorem on Primes in Arithmetic Progressions) *Let a and N be coprime integers. Then there are infinitely many primes p with $p \equiv a \mod N$. Moreover, if $P_{a,N}$ denotes the set of these primes, then for $s \to 1$:*

$$\sum_{p \in P_{a,N}} \frac{1}{p^s} \sim \frac{1}{\varphi(N)} \log \frac{1}{s-1}.$$

Proof. The first statement follows from the second since $\log \frac{1}{s-1} \to \infty$ as $s \to 1$. Consider the (class-)function

$$C_{a,N} : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times \qquad \text{with} \qquad C_{a,N}(n) = \begin{cases} 1, & \text{if } n = a, \\ 0, & \text{else.} \end{cases}$$

Then

$$\langle C_{a,N}, \chi \rangle = \frac{1}{\varphi(N)} \sum_{n \in (\mathbb{Z}/N\mathbb{Z})^\times} C_a(n)\overline{\chi(n)} = \frac{\overline{\chi(a)}}{\varphi(N)},$$

so $C_a = \sum_\chi \frac{\overline{\chi(a)}}{\varphi(N)} \chi$. Hence:

$$\sum_{p \in P_{a,N}} \frac{1}{p^s} = \sum_{p \in \mathbb{P}} C_{a,N}(p)p^{-s} = \sum_{\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} \frac{\overline{\chi(a)}}{\varphi(N)} \sum_p \frac{\chi(p)}{p^s}.$$

By Cor. 44, each term on the RHS is bounded as $s \to 1$ except for $\chi = \mathbf{1}$, and

$$\frac{\overline{\mathbf{1}(a)}}{\varphi(N)} = \sum_p \frac{\mathbf{1}(p)}{p^s} = \frac{1}{\varphi(N)} \sum_{p \nmid N} \frac{1}{p^s} \sim \frac{1}{\varphi(N)} \log(s-1),$$

as $s \to 1$. □

3.4. An Alternative View on Dirichlet characters

Remark We have an isomorphism

$$(\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}), \qquad a \longmapsto \sigma_a \quad \text{with } \sigma_a(\zeta_N) = \zeta_N^a.$$

If $\mathfrak{q}$ is in $\mathbb{Q}(\zeta_N)$ above p then $\sigma_p = \mathrm{Frob}_{\mathfrak{q}/p}$. Thus for any $\mathfrak{q}/p$ we have the correspondence

$$\frac{1}{1 - \psi(p)p^{-s}} \qquad \longleftrightarrow \qquad \frac{1}{1 - \psi(\mathrm{Frob}_{q/p})p^{-s}}.$$

Theorem 46 (Hecke) *Let F/K be a Galois extension of number fields with abelian Galois group* $\mathrm{Gal}(F/K)$ *and a homomorphism* $\psi : \mathrm{Gal}(F/K) \to \mathbb{C}^\times$. *Then*

$$L_*(\psi, s) = \prod_{\substack{\mathfrak{p} \lhd \mathcal{O}_K \\ \textit{unramified in } F/K}} \frac{1}{1 - \psi(\mathrm{Frob}_\mathfrak{p})N(\mathfrak{p})^{-s}}$$

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

Proof. Way beyond the scope of this course. □

Remark When $K = \mathbb{Q}$ and $F = \mathbb{Q}(\zeta_n)$, this recovers Thm. 41.

3.5. Artin L-Functions

Definition Let $I \leq D$ be finite groups and ϱ a D-representation. 06.11.

(*i*) The I-invariant vectors of ϱ are denoted by $\varrho^I = \{v \in \varrho : g(v) = v \ \forall\ g \in I\}$.

(*ii*) If $I \lhd D$ then ϱ^I is a subrepresentation. (If $v \in \varrho^I$, $g \in D$ and $i \in I$, then $i(gv) = (ig)v = gi'v = gv$ for $i' \in I$, so $gv \in \varrho^I$.)

(*iii*) If $\lambda_i \in \mathbb{C}$ and $g_i \in D$, write

$$\det\left(\sum \lambda_i g_i | \varrho\right) := \det_{\varrho}\left(\sum \lambda_i g_i\right).$$

Equivalently, viewing $\varrho : D \to \mathrm{GL}_n(\mathbb{C})$, then

$$\det\left(\sum \lambda_i g_i | \varrho\right) = \det\left(\sum \lambda_i \varrho(g_i)\right),$$

e. g. characteristic polynomial of $g \in D$ on ϱ is $\det(T - g|\varrho)$.

Warning: There is a constant abuse of notation by denoting both the vector space and the homomorphism $D \to \mathrm{GL}_n(\mathbb{C})$ by ϱ.

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

$$P_\mathfrak{p}(F/K, \varrho, T) = P_\mathfrak{p}(\varrho, T) = \det(1 - T \cdot \mathrm{Frob}_\mathfrak{p} | \varrho^{I_\mathfrak{p}}),$$

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

Remark 47 This is essentially the characteristic polynomial $\Phi_{\mathfrak{q}/\mathfrak{p}}(\varrho, T)$ of $\mathrm{Frob}_\mathfrak{p}$ on ϱ: If $P_\mathfrak{p}(\varrho, T) = 1 + a_1 T + a_2 T^2 + \ldots + a_n T^n$, then $\Phi_{\mathfrak{q}/\mathfrak{p}}(\varrho, T) = T^n + a_1 T^{n-1} + a_2 T^{n-2} + \ldots + a_n$. Moreover, if $\dim \varrho = 1$, then:

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

Lemma 48 *The local polynomial $P_\mathfrak{p}(\varrho, T)$ is independent of the choice of $\mathfrak{q}$ and the choice of* $\mathrm{Frob}_\mathfrak{p}$.

Proof. For fixed $\mathfrak{q}$, the independence of choice of $\mathrm{Frob}_\mathfrak{p}$ is clear: two choices differ by an element of $I_\mathfrak{p}$, which acts trivially on $\varrho^{I_\mathfrak{p}}$. If $\mathfrak{q}'$ is a different prime over $\mathfrak{q}$, write $\mathfrak{q}' = g(\mathfrak{q})$ for some $g \in \mathrm{Gal}(F/K)$ and observe that $\mathrm{Frob}'_\mathfrak{p} = g \,\mathrm{Frob}_\mathfrak{p}\, g^{-1}$ is a "lift of the Frobenius for $\mathfrak{q}'/\mathfrak{p}$". The eigenvalues of $\mathrm{Frob}_\mathfrak{p}$ on $\varrho^{I_{\mathfrak{q}'/\mathfrak{p}}} = \varrho^{g I_{\mathfrak{q}\mathfrak{p}} g^{-1}} = g(\varrho^{I_\mathfrak{p}})$ are the same as of $\mathrm{Frob}_\mathfrak{p}$ on $\varrho^{I_\mathfrak{p}}$. Hence their characteristic polynomials agree, and so $P_\mathfrak{p}(\varrho, T)$ is independent of the choice of $\mathfrak{q}$. $\square$

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

$$L(F/K, \varrho, s) = L(\varrho, s) = \prod_{\mathfrak{p} \lhd \mathcal{O}_K} \frac{1}{P_{\mathfrak{p}}(\varrho, N(\mathfrak{p})^{-s})}.$$

The polynomial $P_{\mathfrak{p}}(\varrho, T)$ has form $1 - (a_1 T + a_2 T^2 + \ldots)$, so we can write (ignoring convergence)

$$\frac{1}{P_{\mathfrak{p}}(\varrho, T)} = 1 + (a_1 T + a_2 T^2 + \ldots) + (a_1 T + a_2 T^2 + \ldots)^2 + \ldots = 1 + a_{\mathfrak{p}} T + a_{\mathfrak{p}^2} T^2 + \ldots$$

Formally substituting this into the product gives the expression (*Artin L-series*):

$$L(\varrho, s) = \prod_{\mathfrak{p}} (1 + a_{\mathfrak{p}} N(\mathfrak{p})^{-s} + a_{\mathfrak{p}^2} N(\mathfrak{p})^{-2s} + \ldots) = \sum_{0 \neq \mathfrak{n} \lhd \mathcal{O}_K} a_{\mathfrak{n}} N(\mathfrak{n})^{-s}$$

for suitable $a_{\mathfrak{n}} \in \mathbb{C}$. Note that grouping ideals with equal norm yields an expression for $L(\varrho, s)$ as an ordinary Dirichlet series.

Lemma 49 *The L-series expression for $L(\varrho, s)$ agrees with the Euler product on $\Re(s) > 1$, where they converge absolutely to an analytic function.*

Proof. It suffices to prove that

$$\prod_{\mathfrak{p} \lhd \mathcal{O}_K} \left(1 + a_{\mathfrak{p}} N(\mathfrak{p})^{-s} + a_{\mathfrak{p}^2} N(\mathfrak{p})^{-2s} + \ldots\right)$$

converges absolutely on $\Re(s) > 1$: this justifies rearrangement of terms and the Dirichlet series expression for $L(\varrho, s)$ then proves analyticity (Prop. 37). The polynomial $P_{\mathfrak{p}}(\varrho, T)$ factorises over $\mathbb{C}$ as

$$P_{\mathfrak{p}}(\varrho, T) = (1 - \lambda_1 T)(1 - \lambda_2 T) \cdots (1 - \lambda_k T)$$

for some $k \leq \dim \varrho$ and $|\lambda_i| = 1$. So the coefficients of

$$\frac{1}{P_{\mathfrak{p}}(\varrho, T)} = \frac{1}{\prod (1 - \lambda_i T)} = 1 + a_{\mathfrak{p}} T + a_{\mathfrak{p}^2} T^2 + \ldots$$

are bounded in absolute value by those of

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

Hence:

$$\begin{aligned} \prod_{\mathfrak{p}} \sum_n |a_{\mathfrak{p}^n}| \cdot |N(\mathfrak{p})^{-ns}| &\leq \prod_{\mathfrak{p}} \frac{1}{(1 - |N(\mathfrak{p})^{-ns}|)^{\dim \varrho}} \leq \prod_{\mathfrak{p}} \left(\frac{1}{1 - |p^{-s}|} \right)^{\dim \varrho} \\ &\leq \left(\prod_{p \in \mathbb{P}} \frac{1}{1 - |p^{-s}|} \right)^{\dim \varrho \cdot [K:\mathbb{Q}]} = \zeta(\sigma)^{\dim \varrho \cdot [K:\mathbb{Q}]} < \infty, \end{aligned}$$

where p is the residue character of $\mathfrak{p}$ and $\sigma = \Re(s)$. ☐

Example (*i*) Let $K=\mathbb{Q}$, F arbitrary and $\varrho=\mathbf{1}$. Then 09.11.

$$L(\mathbf{1},s)=\prod_p \frac{1}{1-p^{-s}}=\zeta(s).$$

(*ii*) Let K and F be arbitrary and $\varrho=\mathbf{1}$ then

$$L(F/K,\mathbf{1},s)=\prod_{\mathfrak{p}\lhd\mathcal{O}_K}\frac{1}{1-N(\mathfrak{p})^{-s}}=:\zeta_K(s)$$

is called the *Dedekind ζ-function* of K.

(*iii*) Let $K=\mathbb{Q}$, $F=\mathbb{Q}(\zeta_N)$ and ϱ a 1-dimensional representation of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. Set $\psi:(\mathbb{Z}/N\mathbb{Z})^\times\to\mathbb{C}^\times$ to be $\psi(n)=\varrho(\sigma_n)$, where $\sigma_n(\zeta_N)=\zeta_N^n$. Then

$$\begin{aligned}L(\varrho,s)&=\prod_{p:\varrho(I_p)=1}\frac{1}{1-\varrho(\mathrm{Frob}_p)p^{-s}}=\prod_{p:\varrho(I_p)=1}\frac{1}{1-\psi(p)p^{-s}}\\&=L_N(\psi,s)\prod_{p\mid N,\varrho(I_p)=1}\frac{1}{1-\varrho(\mathrm{Frob}_p)p^{-s}},\end{aligned}$$

e. g. if ϱ is faithful (so $\varrho(I_p)=1$ implies $I_p=\{1\}$) then $L(\varrho,s)=L_N(\psi,s)$.

Proposition 50 *Let F/K be a Galois extension of number fields and ϱ a $\mathrm{Gal}(F/K)$-representation.*

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

$$L(\varrho\oplus\varrho',s)=L(\varrho,s)\cdot L(\varrho',s).$$

(*ii*) *If $N\lhd\mathrm{Gal}(F/K)$ lies in $\ker(\varrho)$, so that ϱ comes from a representation ϱ'' of $\mathrm{Gal}(F/K)/N\cong\mathrm{Gal}(F^N/K)$, then*

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

(*iii*) *Artin Formalism: If $\varrho=\mathrm{Ind}_H^{\mathrm{Gal}(F/K)}\varrho'''$ for a representation ϱ''' of $H\le\mathrm{Gal}(F/K)$, then*

$$L(F/K,\varrho,s)=L(F/F^H,\varrho''',s).$$

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

(*i*) Clear. (Note: $(\varrho\oplus\varrho')^{I_\mathfrak{p}}=\varrho^{I_\mathfrak{p}}\oplus\varrho'^{I_\mathfrak{p}}$.)

(*ii*) We have already proved this – Prop. 34 (for the characteristic polynomial Φ) and Rmk. 47 (for the local polynomial).

(*iii*) Straight from the definitions using the following lemma. □

Lemma 51 (insert as Thm. 28 (vi)–(viii)) *Let F/K be a Galois extension of number fields, $G=\mathrm{Gal}(F/K)$, $N\lhd G$, primes $\mathfrak{p}\lhd\mathcal{O}_K$, $\mathfrak{s}\lhd\mathcal{O}_{F^N}$ and $\mathfrak{q}\lhd\mathcal{O}_F$, where $\mathfrak{q}$ lies above $\mathfrak{s}$ and $\mathfrak{s}$ lies above $\mathfrak{p}$.*

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

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

(iii) *If* $\mathrm{Frob}_\mathfrak{p} \in D_{\mathfrak{q}/\mathfrak{p}}$ *acts as the Frobenius automorphism on* $\mathcal{O}_F/\mathfrak{q}$*, then* $\mathrm{Frob}_\mathfrak{p} N \in D_{\mathfrak{s}/\mathfrak{p}}$ *acts as the Frobenius on* $\mathcal{O}_{F^N}/\mathfrak{s}$.

Proof. (*i*) $D_{\mathfrak{q}/\mathfrak{p}}$ and N both preserve $\mathfrak{s}$, so $D_{\mathfrak{s}/\mathfrak{p}} \geq (D_{\mathfrak{q}/\mathfrak{p}}N)/N$. But

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

(*ii*) Similarly, with e instead of ef.

(*iii*) Clear as $\mathcal{O}_{F^N}/\mathfrak{s}$ is a subfield of $\mathcal{O}_F/\mathfrak{q}$.

□

Theorem 52 *Let F/K be a Galois extension of number fields and ϱ a 1-dimensional* $\mathrm{Gal}(F/K)$*-representation. Then:*

(i) $L(F/K, \varrho, s)$ *has an analytic continuation to* $\mathbb{C}$ *except for a single pole at* $s = 1$ *for* $\varrho = \mathbf{1}$ *(rephrasing Thm. 46).*

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

Proof. By Prop. 50 (ii), we may assume that $F = F^{\ker \varrho}$. In this case ϱ is faithful and $G = \mathrm{Gal}(F/K)$ must be abelian (ϱ maps it isomorphically to a subgroup of $\mathbb{C}^\times$).

(*i*) Is exactly the statement of Thm. 46.

(*ii*) By Prop. 50 (i) and (ii), we have

$$\zeta_F(s) = L(F/K, \mathrm{Ind}_{\{1\}}^G \mathbf{1}, s) = \prod_{\chi \in \hat{G}} L(F/K, \chi, s) = \zeta_K(s) \prod_{\chi \in \hat{G} \setminus \{1\}} L(F/K, \chi, s),$$

where $\hat{G}$ denotes the set of irreducible representations of G. As both ζ-functions have a simple pole at $s = 1$ and each $L(F/K, \chi, s)$ is analytic, it follows that no $L(F/K, \chi, s)$ can have a zero there. □

Example Suppose $\alpha \in \mathcal{O}_K$ and $\alpha \bmod \mathfrak{p}$ is a square in $\mathcal{O}_K/\mathfrak{p}$ for all primes $\mathfrak{p}$ (e.g. $\alpha \in \mathbb{Z}$ with $\alpha \bmod p$ always a square). Claim: α is a square in $\mathcal{O}_K$.

Otherwise by Kummer-Dedekind applied to $X^2 - \alpha$, all $\mathfrak{p} \nmid 2\alpha N$ split in $F = K(\sqrt{\alpha})/K$, where $N = \left[\mathcal{O}_F : \mathcal{O}_K[\sqrt{\alpha}]\right]$. Thus

$$\zeta_F(s) = \prod_{\mathfrak{q} \lhd \mathcal{O}_F} \frac{1}{1 - N(\mathfrak{q})^{-s}} = \prod_{\mathfrak{p} \lhd \mathcal{O}_K,\ \mathfrak{p} \nmid 2N\alpha} \left(\frac{1}{1 - N(\mathfrak{q})^{-s}}\right)^2 \cdot \prod_{\mathfrak{q} \lhd \mathcal{O}_F,\ \mathfrak{q} | 2N\alpha} \frac{1}{1 - N(\mathfrak{q})^{-s}}$$

$$= \zeta_K(s)^2 \cdot \prod_{\mathfrak{q}|2N\alpha} \frac{1}{1-N(\mathfrak{q})^{-s}} \cdot \left(\prod_{\mathfrak{p}\nmid 2N\alpha} \frac{1}{1-N(\mathfrak{q})^{-s}} \right)^{-1}$$

has a simple pole at $s=1$.

Exercise Prove this without ζ-functions.

Example If F/K is cyclic of prime degree p, then infinitely many primes of K remain prime in F: Otherwise $\zeta_F(s) = \zeta_K(s)^p$. Euler factor form ramified and inert primes. By Example Sheet 1, Question 10 there are only finitely many ramified and inert primes. All factors are not equal to 0 or ∞ at $s=1$, so $\zeta_F(s)$ would have a pole of order p.

Exercise Deduce that if $f(X) \in \mathbb{Z}[X]$ is irreducible of prime degree, then $f(X) \bmod p$ is irreducible for infinitely many primes p.

3.6. Induction Theorems

11.11. **Theorem 53** (Artin's Induction Theorem) *Let G be a finite group and ϱ a G-representation. Then for some $n \geq 1$ there are some subgroups $H_i, H_j' \leq G$ and 1-dimensional representations ψ_i, ψ_j' of H_i, H_j', respectively, such that*

$$\varrho^{\oplus n} \oplus \bigoplus_i \operatorname{Ind}_{H_i}^G \psi_i \cong \bigoplus_j \operatorname{Ind}_{H_j'}^G \psi_j'.$$

If $\langle \varrho, \mathbf{1} \rangle = 0$ then all ψ_i, ψ_j' can be chosen to be non-trivial.

Proof.* Write χ_T for the character of T. We begin with the first statment. Let V be the $\mathbb{Q}$-vector space of $\mathbb{Q}$-linear combinations if characters of G (in the space of class functions). Let W be the subspace spanned by $\chi_{\operatorname{Ind}_H^G T}$; for all cyclic $H \leq G$ and 1-dimensional H-representations T. It will suffice to prove that $V = W$, for then $\chi_\varrho = \sum \lambda_i \chi_{\operatorname{Ind}_{H_i} T_i}$, with $\lambda_i \in \mathbb{Q}$. Hence $n\chi_\varrho = \sum k_i \chi_{\operatorname{Ind}_{H_i} T_i}$, with $n, k_i \in \mathbb{Z}$, and so

$$n\chi_\varrho + \sum a_i \chi_{\operatorname{Ind}_{H_i} T_i} = \sum b_j \chi_{\operatorname{Ind}_{H_j} T_j},$$

with $a_i, b_j \in \mathbb{N}$ as required.

Suppose $\psi \in W^\perp$, i.e. $\left\langle \psi, \chi_{\operatorname{Ind}_H^G T} \right\rangle = 0$ for all cyclic H and 1-dimensional T. By Frobenius Reciprocity we have $\left\langle \operatorname{Res}_H^G \psi, \chi_T \right\rangle_H = 0$ for all 1-dimensional T of H. Thus $\operatorname{Res}_H^G \psi = 0$. In particular, taking $H = \langle g \rangle$, shows that $\psi(g) = 0$. This holds for all $g \in G$, so $\psi = 0$. We obtain $W^\perp = 0$, so $V = W$ as claimed.

For the second claim take W to be spanned by $\chi_{\operatorname{Ind}_{H_i}}$ with H cyclic and $T \neq \mathbf{1}$ to be 1-dimensional. It suffices to check that every $\psi \in W^\perp$ isx a multiple of the trivial character. If $\psi \in W^\perp$, by Frobenius Reciprocity we know

$$\langle \psi, \chi_{\operatorname{Ind} T} \rangle = \left\langle \operatorname{Res}_H^G \psi, \chi_T \right\rangle = 0$$

for all cyclic H and 1-dimensional $T \neq \mathbf{1}$. Hence $\operatorname{Res}_H^G \psi$ is a multiple of $\mathbf{1}_H$. Taking $H = \langle g \rangle$ shows that $\psi(g) = \psi(\mathrm{id})$. This is true for all $g \in G$, so ψ is a multiple of $\mathbf{1}_G$. □

Corollary 54 *Let F/K be a Galois extension of number fields and ϱ a* $\mathrm{Gal}(F/K)$*-representation.*

(i) For some $n \geq 1$, $L(\varrho^{\oplus n}, s)$ has a meromorphic continuation to $\mathbb{C}$. If $\langle \varrho, \mathbf{1} \rangle = 0$ it is analytic and non-zero at $s = 1$.

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

Proof. (*i*) For $G = \mathrm{Gal}(F/K)$ write

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

as in Artin's Induction Theorem. It follows from Prop. 50 that on $\Re(s) > 1$ we have

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

By Thm. 52 the RHS has a meromorphic continuation to $\mathbb{C}$. If $\langle \varrho, \mathbf{1} \rangle = 0$ the ψ_i and ψ'_j can be taken to be non-trivial in which case the RHS is also analytic and non-zero at $s = 1$.

(*ii*) $L(\varrho, s)^n$ is analytic and non-zero at $s = 1$ for some n. On $\Re(s) > 1$ the function $L(\varrho, s)$ is an analytic branch of the n^{th} root of $L(\varrho, s)^n$, and hence has an analytic continuation to $s = 1$ (this not being a branch point). □

Theorem (Brauer's Induction Theorem*) *Let G be a finite group and ϱ a G-representation. Then there are elementary subgroups (i. e. products of cyclic and p-groups) $H_i, H'_j \leq G$ and 1-dimensional representations ψ_i, ψ'_j of H_i, H'_j respectively, such that*

$$\varrho \oplus \bigoplus_i \operatorname{Ind}_{H_i} \psi_i \cong \bigoplus_j \operatorname{Ind}_{H'_j} \psi'_j.$$

Corollary (Artin-Brauer*) *$L(\varrho, s)$ has a meromorphic continuation to $\mathbb{C}$.*

Theorem (Solomon's Induction Theorem*) *Let G be a finite group. There are soluble (in fact quasi-elementary) subgroups H_i, H'_j, such that:*

$$\mathbf{1} \oplus \bigoplus_i \operatorname{Ind}_{H_i}^G \mathbf{1} \cong \bigoplus_j \operatorname{Ind}_{H'_j}^G \mathbf{1}.$$

3.7. Density Theorems

Definition Let S be a set of primes. Then S has *Dirichlet density* α if 13.11.

$$\lim_{s\searrow 1} \frac{\sum_{p\in M} p^{-s}}{\log \frac{1}{s-1}} = \alpha.$$

Example (*i*) The set of all primes has density 1 (rather by Euler than by Dirichlet).

(*ii*) The set $\mathbb{P}_{a,N} = \{p \in \mathbb{P} : p \equiv a \mod N\}$ has density $1/\varphi(N)$ whenever $\gcd(a, N) = 1$.

Definition For $F/\mathbb{Q}$ Galois, p a prime of $\mathbb{Q}$ unramified in F, write $\mathrm{Frob}_p \in \mathrm{Gal}(F/\mathbb{Q})$ for the Frobenius element $\mathrm{Frob}_{\mathfrak{q}/p}$ for some prime $\mathfrak{q} \lhd \mathcal{O}_F$ above p. Note that it lies in a well defined conjugacy class of $\mathrm{Gal}(F/\mathbb{Q})$ as $\mathrm{Frob}_{\mathfrak{q}'/p} = x\,\mathrm{Frob}_{\mathfrak{q}/p}\,x^{-1}$ for $\mathfrak{q}' = \mathfrak{q}^x$.

Example Let $F = \mathbb{Q}(\zeta_N)$ and $\sigma_a \in \mathrm{Gal}(F/\mathbb{Q})$ with $\sigma_a(\zeta_N) = \zeta_N^a$. For $p \nmid N$ we have $\mathrm{Frob}_p = \sigma_a$ iff $p \equiv a \mod N$ (as $\mathrm{Frob}_p(\zeta_N) \equiv \zeta_N^p \mod \mathfrak{q}$ and hence $\mathrm{Frob}_p(\zeta_N) = \zeta_N^p$). So Dirichlet's Theorem shows that $\mathbb{P}_{N,\sigma} = \{p \nmid N : \mathrm{Frob}_p = \sigma\}$ has Dirichlet density $|\mathrm{Gal}(F/\mathbb{Q})|^{-1}$, i. e. Frob_p are "uniformly distributed" among $\mathrm{Gal}(F/\mathbb{Q})$.

Theorem 55 (Chebotarev's Density Theorem) *Let $F/\mathbb{Q}$ be a finite Galois extension and $\mathcal{C}$ a conjugacy class of $\mathrm{Gal}(F/\mathbb{Q})$. Then*

$$\mathbb{P}_{\mathcal{C}} = \{p \in \mathbb{P} : p \textit{ unramified in } F/\mathbb{Q} \textit{ s. t. } \mathrm{Frob}_p \in \mathcal{C}\}$$

has Dirichlet density $|\mathcal{C}|/|\mathrm{Gal}(F/\mathbb{Q})|$.

Proof. For ϱ a representation of $\mathrm{Gal}(F/\mathbb{Q})$ let

$$L_*(\varrho, s) = \prod_{p \text{ unram.}} P_p(\varrho, p^{-s})^{-1}.$$

By Example Sheet 1, Question 10 only finitely many primes ramify in $F/\mathbb{Q}$, so by Cor. 54 we know that $L_*(\varrho, s)$ has neither a pole nor a zero at $s = 1$ if $\varrho \neq \mathbf{1}$ irreducible, but $L_*(\varrho, s)$ has a simple pole at $s = 1$ for $\varrho = \mathbf{1}$. Now write χ_ϱ for the character of ϱ. If p is unramified in $F/\mathbb{Q}$ (which implies $\varrho = \varrho^{I_p}$) and $\lambda_1, \ldots, \lambda_d$ are the eigenvalues (with multiplicity) of Frob_p on ϱ. Then

$$\begin{aligned}\log \frac{1}{P_p(\varrho, p^{-s})} &= \log \frac{1}{\prod_i (1 - \lambda_i p^{-s})} = \sum_i \log \frac{1}{1 - \lambda_i p^{-s}} \\ &= \sum_i \lambda_i p^{-s} + \frac{1}{2} \sum_i \lambda_i^2 p^{-2s} + \ldots = \sum_{n \geq 1} \frac{\chi_\varrho(\mathrm{Frob}_p^n)}{n} p^{-ns}.\end{aligned}$$

The Dirichlet series

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

has bounded coefficients, so defines an analytic branch of $\log L_*(\varrho, s)$ on $\Re(s) > 1$ (by proof of Prop. 43). Now the series is bounded on $\Re(s) > 1$ by $2 \dim \varrho \sum \frac{1}{k^2}$ (see proof of Cor. 44). So by using the definition we obtain that

$$f_\varrho(s) = \sum_{p \text{ unram.}} \chi_p(\mathrm{Frob}_p) p^{-s}$$

is bounded as $s \to 1$ on $\Re(s) > 1$ if $\varrho \neq \mathbf{1}$ is irreducible and

$$f_{\mathbf{1}}(s) = \sum_{p \text{ unram.}} p^{-s} \sim \log \frac{1}{s-1}$$

as $s \to 1$. Finally, let $\mathrm{I}_{\mathcal{C}}(g)$ be 1 if $g \in \mathcal{C}$ and 0 else. Then

$$\begin{aligned}\sum_{p \in \mathbb{P}_{\mathcal{C}}} p^{-s} = \sum_{p \text{ unram.}} \mathrm{I}_{\mathcal{C}}(\mathrm{Frob}_p) p^{-s} &= \sum_{p} \langle \chi_p, \mathrm{I}_{\mathcal{C}} \rangle f_{\varrho}(s) \\ &= \frac{|\mathcal{C}|}{|\operatorname{Gal}(F/\mathbb{Q})|} f_{\mathbf{1}}(s) + \sum_{\varrho \neq \mathbf{1}} \langle \chi_p, \mathrm{I}_{\mathcal{C}} \rangle f_p(s).\end{aligned}$$

Hence $\mathbb{P}_{\mathcal{C}}$ has Dirichlet density $\frac{|\mathcal{C}|}{|\operatorname{Gal}(F/\mathbb{Q})|}$. □

Corollary 56 *Let $f \in \mathbb{Z}[X]$ be a monic irreducible polynomial and $G = \operatorname{Gal}(f)$ the Galois group of the splitting field of f. Then the set of primes p, such that $f \bmod p$ factorises as a product of irreducible polynomials of degree $d_1, \ldots, d_r$ has density*

$$\frac{|\{g \in G : g \textit{ has cycle type } (d_1, \ldots, d_r) \textit{ on the roots of } f\}|}{|G|}.$$

Proof. The polynomial $f \bmod p$ has a repreated root (in $\mathbb{F}_p$) modulo finitely many primes p (these divide $\operatorname{disc} f$, the discriminant). For the rest, Frob_p acts as an element of cylce type $(d_1, \ldots, d_r)$ where these are the degrees of the irreducible factors of $f \bmod p$. □

Example Let f be an irreducible quintic polynomial with Galois group S_5. Then:

(i) The primes p, such that f split into linear factors $\bmod p$ have density $\frac{1}{120}$.

(ii) The primes p, such that $f \bmod p$ is irreducible have density $\frac{1}{120} \cdot \#\{5 \text{ cycles in } S_5\} = \frac{1}{5}$.

(iii) The primes p, such that $f \bmod p$ splits into a product of a quadratic and a cubic have density $\frac{20}{120} = \frac{1}{6}$.

Corollary 57 *If $f \in \mathbb{Z}[X]$ is irreducible and monic with $\deg f > 1$, then $f \bmod p$ has no root in $\mathbb{F}_p$ for infinitely many primes p.*

Proof. It is sufficient to prove that there exists a $g \in \operatorname{Gal}(f)$ that fixes no root of f. Let $G = \operatorname{Gal}(f)$. Then $|G_\alpha| = |G|/\deg f$ (orbit-stabiliser) and each stabiliser contains the identity, so

$$\left| \bigcup_{\alpha \text{ root}} G_\alpha \right| < \deg f \cdot \frac{|G|}{\deg f}.$$

Hence there is $g \in G$, that fixes no root α. □

4. Class Field Theory

4.1. The Frobenius Element

16.11. **Definition** An extension F/K is *abelian* if it is Galois and $\mathrm{Gal}(F/K)$ is abelian. Let F/K be abelian and $\mathfrak{p} \lhd \mathcal{O}_K$ a prime of K unramified in F/K. Write $\mathrm{Frob}_\mathfrak{p} = \mathrm{Frob}_\mathfrak{p}(F/K) = \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ for any prime $\mathfrak{q} \lhd \mathcal{O}_F$ of F above $\mathfrak{p}$. Note that this is a well-defined element of $\mathrm{Gal}(F/K)$. A different $\mathfrak{q}$ would yield a conjugate element, but $\mathrm{Gal}(F/K)$ is abelian.

Remark 58 Note that $\mathfrak{p}$ (unramified) splits completely iff $\mathrm{Frob}_\mathfrak{p} = \mathrm{id}$ (or equivalently iff $f_\mathfrak{p} = 1$). Note also that if $F/L/K$ is an intermediate field, then $\mathrm{Frob}_\mathfrak{p}(L/K)$ is the image of $\mathrm{Frob}_\mathfrak{p}(F/K)$ under the projection $\mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K)$ (cf. Lemma 51 (iii)). In particular, $\mathfrak{p}$ splits completely in L iff $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(F/L)$.

4.2. Cyclotomic Extensions

Definition An extension F/K is called *cyclotomic* if there is $N \geq 1$ such that $F \subseteq K(\zeta_N)$, where ζ_N is a primitive N^{th} root of unity. Note that cyclotomic extensions are abelian:

$$\mathrm{Gal}(K(\zeta_N)/K) \leq (\mathbb{Z}/N\mathbb{Z})^\times.$$

Lemma 59 *Let $F = K(\zeta_N)$ and $\mathfrak{p} \nmid N$ a prime of K. Then $\mathfrak{p}$ is unramified in F and* $\mathrm{Frob}_\mathfrak{p}$ *is the unique element with* $\mathrm{Frob}_\mathfrak{p}(\zeta_N) = \zeta_N^{N(\mathfrak{p})}$.

Proof. The polynomial $X^N - 1$ has no repeated roots in characteristic $p \nmid N$ (being coprime to $\frac{\mathrm{d}}{\mathrm{d}X}(X^N - 1)$). Let $\mathfrak{q}$ in F be a prime above $\mathfrak{p}$. Then $I_{\mathfrak{q}/\mathfrak{p}}$ fixes each $\zeta_N \bmod \mathfrak{q}$ (by definition), and hence can only contain the identity element (as $\zeta_N \bmod \mathfrak{q}$ are distinct). Thus $\mathfrak{p}$ is unramified. By $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}(\zeta_N) \equiv \zeta_N^{N(\mathfrak{p})} \mod \mathfrak{q}$ we obtain $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}(\zeta_N) = \zeta_N^{N(\mathfrak{p})}$ (this being the only N^{th} root of unity with reduction modulo $\mathfrak{q}$). $\square$

Lemma 60 *Let $F = \mathbb{Q}(\zeta_N)$.*

(i) A prime p ramifies in $F/\mathbb{Q}$ iff $p \mid N$.

(ii) A prime p splits completely in $F/\mathbb{Q}$ iff $p \equiv 1 \mod N$.

(iii) We have $\mathrm{Frob}_{p_1} = \mathrm{Frob}_{p_2}$ *iff $p_1 \equiv p_2 \mod N$, where $p_1, p_2 \nmid N$.*

(iv) For primes p_i, p'_j with $p_i, p'_j \nmid N$ we have:

$$\prod_i \mathrm{Frob}_{p_i} = \prod_j \mathrm{Frob}_{p'_j} \qquad \Longleftrightarrow \qquad \prod_i p_i \equiv \prod_j p'_j \mod N.$$

(v) The map

$$\varphi : \left\{\tfrac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{N},\ (a, N) = (b, N) = 1\right\} \longrightarrow \mathrm{Gal}(F/\mathbb{Q}),$$
$$\tfrac{\prod p_i}{\prod p'_j} \longmapsto \left(\prod \mathrm{Frob}_{p_i}\right) \left(\prod \mathrm{Frob}_{p'_j}\right)^{-1}$$

is a surjective homomorphism with kernel $\left\{\frac{a}{b} : a \equiv b \mod N\right\}$.

Proof. (*i*) By Lemma 59 and second example after Thm. 20.

(*ii*) p splits completely iff $p \nmid N$ and $\mathrm{Frob}_p = \mathrm{id}$ iff $p \nmid N$ and $\zeta_N^p = \zeta_N$ iff $p \equiv 1 \mod N$.

(*iii*) Straight from (iv).

(*iv*) $\left(\prod \mathrm{Frob}_{p_i}\right)(\zeta_N) = \zeta_N^{\prod p_i}$ and similarly for p'_j.

(*v*) This is clearly a well-defined homomorphism. The kernel is correct by (iv). The map is surjective by Dirichlet's Theorem on Primes in Arithmetic Progressions. □

Theorem 61 *Let $F/\mathbb{Q}$ cyclotomic with $F = \mathbb{Q}(\zeta_N)^H$.*

(i) There is $N \geq 1$ and $H \leq (\mathbb{Z}/N\mathbb{Z})^\times$ such that:

(a) A prime p with $p \nmid N$ splits completely in F iff $p \bmod N \in H$.

(b) For primes p_i, p'_j with $p_i, p'_j \nmid N$ we have:

$$\prod_i \mathrm{Frob}_{p_i} = \prod_j \mathrm{Frob}_{p'_j} \qquad \Longleftrightarrow \qquad \frac{\prod p_i}{\prod p'_j} \in H.$$

(c) The map

$$\varphi : \left\{\tfrac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{N},\ (a, N) = (b, N) = 1\right\} \longrightarrow \mathrm{Gal}(F/\mathbb{Q}),$$
$$\tfrac{\prod p_i}{\prod p'_j} \longmapsto \left(\prod \mathrm{Frob}_{p_i}\right) \left(\prod \mathrm{Frob}_{p'_j}\right)^{-1}$$

is a surjective homomorphism with kernel $\left\{\frac{a}{b} \bmod N \in H\right\}$.

(ii) There is a least N that works; any other N' will have $N \mid N'$. For this N we have $p \mid N$ iff p ramifies in F.

(iii) For every $N \geq 1$ and $H \leq (\mathbb{Z}/N\mathbb{Z})^\times$ there is a unique cyclotomic field giving rise to (N, H) as above.

Proof. (*i*) If $F = \mathbb{Q}(\zeta_N)^H$ take these N and H.

(a) Follows from Remark 58 and Lemma 59.

(b) Ditto.

(c) Follows from (b) and Lemma 60 (v).

(ii) If N_1 and N_2 both work, then $\varphi(x) = \varphi(y)$ for $x \equiv y \mod \gcd(N_1, N_2)$. So we can take $N = \gcd(N_1, N_2)$ as well. Assuming (iii) we have $F = \mathbb{Q}(\zeta_N)^H$, so p ramifies iff $\mathbb{Q}(\zeta_N)^H \nsubseteq \mathbb{Q}(\zeta_m)$ for any m coprime to p (exercise).

(iii) Take $F = \mathbb{Q}(\zeta_N)^H$. Uniqueness: If $F_1 \neq F_2$ with $F_1, F_2 \subseteq \mathbb{Q}(\zeta_{NM})$ then $F_i = \mathbb{Q}(\zeta_{NM})^{H_i}$ with $H_1 \neq H_2$. Thus different primes split completely in F_1 and F_2. □

18.11. **Example** (i) Let $F = \mathbb{Q}(\zeta_7)$, $N = 7$, $(\mathbb{Z}/N\mathbb{Z})^\times \cong C_6$ and $H = \{1\}$. Then the primes that split completely in $F/\mathbb{Q}$ are $p \equiv 1 \mod 7$; the only ramified prime is 7. For the Frobenius elements we have $\mathrm{Frob}_2 = \mathrm{Frob}_{23} = \mathrm{Frob}_{37} = (\mathrm{Frob}_3)^2$ etc.

(ii) Let $F = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_7)^H$, $N = 7$ and $H = \{1, 2, 4\} \cong C_3$ (the squares in $(\mathbb{Z}/7\mathbb{Z})^\times$). Then the primes that split completely in $F/\mathbb{Q}$ are $p \equiv 1, 2, 4 \mod 7$; the only ramified prime is 7. For the Frobenius elements we have $\mathrm{Frob}_2 = \mathrm{Frob}_{11} = \mathrm{Frob}_{29} = \mathrm{Frob}_3 \cdot \mathrm{Frob}_{15} = \mathrm{id}$ etc. and $\mathrm{Frob}_3 = \mathrm{Frob}_5 = \mathrm{Frob}_{17} = (\mathrm{Frob}_3)^3$, which is the complex conjugation.

Proposition 62 *Let $F = K(\zeta_N)$.*

(i) If $\mathfrak{p} = (\alpha)$ is a prime of K with $\alpha \equiv 1 \mod N$ and $\sigma(\alpha) > 0$ for each real embedding $\sigma : K \hookrightarrow \mathbb{R}$ then $\mathfrak{p}$ splits completely in F/K.

(ii) Define

$$\varphi : \bigoplus_{\mathfrak{p} \nmid N} \mathfrak{p}^{\mathbb{Z}} \longrightarrow \mathrm{Gal}(F/K)$$

by $\varphi(\mathfrak{p}) = \mathrm{Frob}_{\mathfrak{p}}$. This gives a homomorphism whose kernel contains

$$P_N^1 = \left\{ (\alpha)(\beta)^{-1} : \alpha \equiv \beta \mod N,\ \sigma\left(\frac{\alpha}{\beta}\right) > 0\ \forall\, \sigma : K \hookrightarrow \mathbb{R} \right\}.$$

Equivalently: if $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$ with $\alpha \equiv \beta \mod N$ and $\sigma\left(\frac{\alpha}{\beta}\right) > 0$ for all embeddings σ then $\varphi(\mathfrak{a}) = \varphi(\mathfrak{b})$.

Proof. (i) If $\alpha = 1 + Nt$ with $t \in \mathcal{O}_K$ then

$$N(\alpha) = \prod_{\sigma : K \hookrightarrow \mathbb{C}} \sigma(\alpha) = \prod_{\sigma : K \hookrightarrow \mathbb{C}} (1 + N\sigma(t)) = 1 + N\lambda,$$

where λ is an algebraic integer in $\mathbb{Q}$, i. e. $\lambda \in \mathbb{Z}$. Moreover $\sigma(1 + Nt) > 0$ for all embeddings $\sigma : K \hookrightarrow \mathbb{R}$ and $\sigma(1 + Nt)\bar{\sigma}(1 + Nt) > 0$ for all pairs $\sigma, \bar{\sigma}$ of complex conjugates. Thus $N(\alpha) > 0$ and so

$$N((\alpha)) = |N(\alpha)| = N(\alpha) = 1 + N\lambda \equiv 1 \mod N.$$

Hence $\mathrm{Frob}_{\mathfrak{p}}(\zeta_N) = \zeta_N^{N(\mathfrak{p})} = \zeta_N^{1+N\lambda} = \zeta_N$ and so $\mathfrak{p}$ splits completely.

(*ii*) Similarly, if $\alpha = k + Nt$, then $N(\alpha) = N(k) + N\lambda$ with $\lambda \in \mathbb{Z}$. So $\alpha \equiv \beta \mod N$ and hence $N(\alpha) \equiv N(\beta) \mod N$. If also $\sigma\big(\frac{\alpha}{\beta}\big) > 0$ for all σ then $N\big(\frac{\alpha}{\beta}\big) > 0$ and so $N((\alpha)) \equiv N((\beta)) \mod N$. Thus we have $\zeta_N^{N((\alpha))} = \zeta_N^{N((\beta))}$. $\square$

Example Let $K = \mathbb{Q}(i)$, and $F = K(\zeta_3)$. Then $\mathcal{O}_K = \mathbb{Z}[i]$ is a UFD. If $\mathfrak{q} = (\alpha)$ with $\alpha = 1 + 3t$, $t \in \mathbb{Z}[i]$, then

$$N(\alpha) = (1 + 3t)(\overline{1 + 3t}) = 1 + 3(t + \bar{t}) + 9t\bar{t} \equiv 1 \mod 3,$$

so $\zeta_3^{N((\alpha))} = \zeta_3^{N(\alpha)} = \zeta_3$. Other cases:

$$\begin{aligned}
N(2 + 3t) &= 4 + 3(\dots) \equiv 1 \mod 3,\\
N(i + 3t) &= i(-i) + 3(\dots) \equiv 1 \mod 3,\\
N(2i + 3t) &= 4 + 3(\dots) \equiv 1 \mod 3,\\
N((1 + i) + 3t) &= (1 + i)(1 - i) + 3(\dots) \equiv 2 \mod 3,\\
N((1 + 2i) + 3t) &= 5 + 3(\dots) \equiv 2 \mod 3,\\
N((2 + 2i) + 3t) &= 8 + 3(\dots) \equiv 2 \mod 3.
\end{aligned}$$

So let $\mathfrak{p} = (\alpha)$. If $\alpha \equiv \pm 1, \pm i \mod 3$ then $\mathrm{Frob}_{\mathfrak{p}} = \mathrm{id}$; if $\alpha \equiv \pm 1 \pm i \mod 3$ then $\mathrm{Frob}_{\mathfrak{p}} : \zeta_3 \mapsto \zeta_3^{-1}$. Now let $\mathfrak{a} = \prod \mathfrak{p}_i = (\alpha)$. If $\alpha \equiv \pm 1, \pm i \mod 3$ then $\prod \mathrm{Frob}_{\mathfrak{p}_i} = \mathrm{id}$; if $\alpha \equiv \pm 1 \pm i \mod 3$ then $\prod \mathrm{Frob}_{\mathfrak{p}_i} : \zeta_3 \mapsto \zeta_3^{-1}$. Note that $(\alpha) = (-\alpha) = (i\alpha) = (-i\alpha)$, so ± 1 and $\pm i$ must give equal $\mathrm{Frob}_{\mathfrak{p}}$, and similar for $\pm 1 \pm i$.

Example Let $K = \mathbb{Q}\big(\sqrt{-5}\big)$ with $\mathcal{O}_K = \mathbb{Z}\big[\sqrt{-5}\big]$, and $F = K(\zeta_3)$. The residues modulo 3 are ± 1, $\pm\sqrt{-5}$, $\pm 1 \pm \sqrt{-5}$, and 0. Of these, $\pm 1 \pm \sqrt{-5}$ are not coprime to (3). (Note that $(3) = \mathfrak{p}_3\mathfrak{p}_3' = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$ in $\mathcal{O}_K$, so $\mathcal{O}_K/(3) \cong \mathbb{F}_3 \times \mathbb{F}_3$ and $(\mathcal{O}_K/(3))^\times \cong C_2 \times C_2$.) We have

$$N(\pm 1 + 3t) \equiv 1 \mod 3, \qquad \text{and} \qquad N(\pm\sqrt{-5} + 3t) \equiv 2 \mod 3.$$

So let $\mathfrak{p} = (\alpha)$ prime. If $\alpha \equiv \pm 1 \mod 3$ then $\mathrm{Frob}_{\mathfrak{p}} = \mathrm{id}$; if $\alpha \equiv \pm\sqrt{-5} \mod 3$ then $\mathrm{Frob}_{\mathfrak{p}} : \zeta_3 \mapsto \zeta_3^{-1}$. But $\mathcal{C}\ell_K = C_2$, so what about non-principal ideals? Take $\mathfrak{p}_2 = (2, 1 + \sqrt{-5})$, the prime above 2. As $\mathfrak{p}_2^2 = (2)$, we have $N(\mathfrak{p}_2)^2 = N(\mathfrak{p}_2^2) = 4$, and so $N(\mathfrak{p}_2) = 2$. Hence $\mathrm{Frob}_{\mathfrak{p}_2} : \zeta_3 \mapsto \zeta_3^2 = \zeta_3^{-1}$. If $\mathfrak{p}$ is non-principal then $\mathfrak{p}\mathfrak{p}_2$ is, so $\mathfrak{p}\mathfrak{p}_2 = (\alpha)$. Thus

$$\mathrm{Frob}_{\mathfrak{p}} = \begin{cases} \mathrm{id}, & \alpha \equiv \pm\sqrt{-5} \mod 3,\\ \zeta_3 \mapsto \zeta_3^{-1}, & \alpha \equiv \pm 1 \mod 3, \end{cases}$$

i. e. $\mathrm{Frob}_{\mathfrak{p}}$ is determined by the image of $\mathfrak{p}$ in the ideals modulo prime ideals that are congruent to 1 modulo 3 (this is isomorphic to $C_2 \times C_2$).

4.3. Class Fields

Definition Let K be a number field. A *modulus* $\mathfrak{m}$ is a formal product of an ideal of $\mathcal{O}_K$ and some real embeddings ("real places") of K:

$$\mathfrak{m} = \prod_i \mathfrak{p}_i^{n_i} \prod_j \sigma_j = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty.$$

Write

$$I_{\mathfrak{m}} = \bigoplus_{\mathfrak{p} \nmid \mathfrak{m}_0} \mathfrak{p}^{\mathbb{Z}}$$

for the group of fractional ideals coprime to $\mathfrak{m}_0$, and $P^1_{\mathfrak{m}}$ for the ideals of the form
20.11. $(\alpha)(\beta)^{-1}$ with $\alpha \equiv \beta \mod \mathfrak{m}_0$ and $\sigma\left(\frac{\alpha}{\beta}\right) > 0$ for all $\sigma \mid \mathfrak{m}_\infty$. Set $P_{\mathfrak{m}_0}$ to be the subgroup generated by the principal ideals coprime to $\mathfrak{m}_0 = \{(\alpha)(\beta)^{-1}\}$ and $P_{\mathfrak{m}}$ to be the principal ideals with $\sigma\left(\frac{\alpha}{\beta}\right) > 0$ for all $\sigma \mid \mathfrak{m}_\infty$.

Remark Note $I_{\mathfrak{m}} = I_{\mathfrak{m}_0}$. We have:

$$I_{\mathfrak{m}}/P_{\mathfrak{m}} = \frac{I_{\mathfrak{m}}}{P_{\mathbf{1}} \cap I_{\mathfrak{m}}} = \frac{I_{\mathfrak{m}} P_{\mathbf{1}}}{P_{\mathbf{1}}} \leq \mathcal{C}\ell_K,$$

where $P_{\mathbf{1}}$ are the principal ideals. In fact we have equality. Moreover $P_{\mathfrak{m}_0}/P_{\mathfrak{m}}$ is a subgroup of $\mathbb{Z}/2\mathbb{Z}^{\#\sigma|\mathfrak{m}_\infty}$ (again it is in fact equality). We have an isomorphism $P_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong (\mathcal{O}_K/\mathfrak{m}_0)^\times/\mathcal{O}_K^\times$ via $(\alpha) \mapsto \alpha \bmod \mathfrak{m}_0$. Thus $I_{\mathfrak{m}}/P^1_{\mathfrak{m}}$ is finite.

Definition A *congruence subgroup* H for $\mathfrak{m}$ is a subgroup of $I_{\mathfrak{m}}$ containing $P^1_{\mathfrak{m}}$. An extension F/K is a *class field* for $(\mathfrak{m}, H)$ if the primes $\mathfrak{p} \nmid \mathfrak{m}$ of K that split completely in F are exactly those that lie in H.

Example Let $K = \mathbb{Q}$.

(*i*) Take $\mathfrak{m} = N \cdot \infty$, where ∞ is the unique embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$. Then

$$I_{\mathfrak{m}} = \left\{ \frac{\prod \mathfrak{p}_i}{\prod \mathfrak{p}'_j} : \mathfrak{p}_i,\, \mathfrak{p}'_j \text{ coprime to } N \right\} \cong \left\{ \frac{a}{b} : a, b \in \mathbb{N} \text{ coprime to } N \right\},$$

and $P^1_{\mathfrak{m}}$ is the subgroup generated by $\frac{(a)}{(b)}$ with $a \equiv b \mod N$, and $\frac{a}{b} > 0$ (equivalently to $\alpha \equiv 1 \mod N$, where $\alpha \in \mathbb{Q}_{>0}$). Then we have $I_{\mathfrak{m}}/P^1_{\mathfrak{m}} = (\mathbb{Z}/N\mathbb{Z})^\times$.

(*ii*) Take $\mathfrak{m} = N$. Then $P^1_{\mathfrak{m}}$ is the subgroup generated by (a) with $a \equiv 1 \mod N$, and $I_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$.

(*iii*) Take $\mathfrak{m} = 5 \cdot \infty$. Then $H = P^1_{\mathfrak{m}}$ has field $\mathbb{Q}(\zeta_5)$. Now let $P^1_{\mathfrak{m}} \leq H \leq I_{\mathfrak{m}}$ be of index 2. Then H has class field $\mathbb{Q}(\sqrt{5})$. (Note that H is given by $\{1, 4\} \leq (\mathbb{Z}/5\mathbb{Z})^\times = I_{\mathfrak{m}}/P^1_{\mathfrak{m}}$.)

Example (*i*) Let $K = \mathbb{Q}(i)$ and $\mathfrak{m} = (3)$. Then $I_{\mathfrak{m}}$ are the (fractional) ideals coprime to 3, and $P^1_{\mathfrak{m}}$ are those ideals generated by $\alpha \equiv 1 \mod 3$. So $I_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong (\mathbb{Z}[i]/(3))^\times/\{\pm 1, \pm i\} \cong C_2$, and $F = K(\zeta_3)$ is a class field for $(\mathfrak{m}, P^1_{\mathfrak{m}})$.

(*ii*) Let $K = \mathbb{Q}(\sqrt{-5})$ and $\mathfrak{m} = (3) = \mathfrak{p}_3\mathfrak{p}'_3$. Since $\mathfrak{p}_2$ is a non-principal prime ideal above 2, we have

$$I_{\mathfrak{m}}/P^1_{\mathfrak{m}} \cong C_2 \times C_2 = \left\langle [\mathfrak{p}_2], [\sqrt{-5}] \right\rangle.$$

Take $H = \left\{ \mathrm{id}, [\mathfrak{p}_2(\sqrt{-5})] \right\}$. Then $F = K(\zeta_3)$ is a class field for $(\mathfrak{m}, H)$.

4.4. The Main Theorem of Class Field Theory

Theorem 63 (Takagi-Artin) *Let K be a number field.*

(i) Every abelian extension F/K is a class field for some $(\mathfrak{m}, H)$.

(ii) Every $(\mathfrak{m}, H)$ has a unique class field F. Moreover F is abelian over K.

(iii) Among $(\mathfrak{m}, H)$ in (i) there is a minimal one, in the sense that other $(\mathfrak{m}', H')$ have $\mathfrak{m} \mid \mathfrak{m}'$. The minimal modulus $\mathfrak{m}$ is called the conductor of F/K. The primes that ramify in F/K are precisely those that divide the conductor; moreover the real embeddings in the conductor are precisely those that extend to complex embeddings in F.

(iv) Artin Reciprocity Law: If F/K is a class field for $(\mathfrak{m}, H)$ then the Artin map

$$\varphi : I_{\mathfrak{m}}/P_{\mathfrak{m}}^1 \longrightarrow \mathrm{Gal}(F/K), \qquad \varphi(\mathfrak{p}) := \mathrm{Frob}_{\mathfrak{p}},$$

is a surjective homomorphism with kernel H.

Proof. Beyond the scope of this course. □

Corollary 64 (Kronecker-Weber Theorem) *All abelian extensions of $\mathbb{Q}$ are cyclotomic.*

Proof. By Thm. 61, cyclotomic fields are class fields for all possible moduli $\mathfrak{m} = N \cdot \infty$ and congruence subgroups H. So by uniqueness (in (ii)) and (iii) they exhaust all abelian extensions which are imaginary (so no subset of $\mathbb{R}$). Hence a general abelian extension $F/\mathbb{Q}$ has $F(i)$ cyclotomic, so F is cyclotomic as well. □

Lemma 65 *Let $\mathfrak{m} = \mathfrak{m}_0 = \prod_i \mathfrak{p}_i^{n_i}$ be an ideal of $\mathcal{O}_K$, with $\mathfrak{p}_i$ distinct primes.* 23.11.

(i) We have an isomorphism

$$(\mathcal{O}_K/\mathfrak{m})^\times/\mathcal{O}_K^\times \xrightarrow{\sim} P_{\mathfrak{m}}/P_{\mathfrak{m}}^1, \qquad \alpha \longmapsto (\alpha),$$

where $P_{\mathfrak{m}}$ is the subgroup of $I_{\mathfrak{m}}$ generated by principal ideals.

(ii) We have an isomorphism

$$(\mathcal{O}_K/\mathfrak{m})^\times \xrightarrow{\sim} \prod_i (\mathcal{O}_K/\mathfrak{p}_i^{n_i})^\times, \qquad x \longmapsto (x \bmod \mathfrak{p}_1^{n_1}, \dots, x \bmod \mathfrak{p}_r^{n_r}).$$

(iii) If $\mathfrak{p}$ is prime then $(\mathcal{O}_K/\mathfrak{p}^n)^\times \cong C_{p^k-1} \times A$, where $p^k = N(\mathfrak{p})$ and A is an abelian group of order $p^{k(n-1)}$.

Proof. (*i*) Let $\psi : (\mathcal{O}_K/\mathfrak{m})^\times \to P_{\mathfrak{m}}/P_{\mathfrak{m}}^1$ by $\psi(\alpha) = (\alpha)$. Then ψ is well-defined: if $\alpha \equiv \beta \mod \mathfrak{m}$ then $(\alpha)(\beta)^{-1} \in P_{\mathfrak{m}}^1$ by definition. For the kernel we see that $(\alpha) \in P_{\mathfrak{m}}^{-1}$ iff there is $\beta \equiv \gamma \mod \mathfrak{m}$ with $(\alpha) = (\beta)(\gamma)^{-1}$ iff there is $\delta \equiv 1 \mod \mathfrak{m}$ such that $(\alpha) = (\delta)$ iff there is $u \in \mathcal{O}_K^\times$ such that $\alpha \equiv u \mod \mathfrak{m}$. Hence $\ker \psi = \mathcal{O}_K^\times \mod \mathfrak{m}$. Moreover, if β and γ are coprime to $\mathfrak{m}$, pick $\delta \in \mathcal{O}_K$ such that $\gamma\delta \equiv 1 \mod \mathfrak{m}$ by the Chinese Remainder Theorem (Thm. 12). Then

$$\psi(\beta\delta) = (\beta\delta) = (\beta)(\gamma)^{-1}(\gamma\delta) = (\beta)(\gamma)^{-1}(P_{\mathfrak{m}})^{-1},$$

thus ψ is surjective.

(*ii*) This follows from the Chinese Remainder Theorem (Thm. 12).

(*iii*) By unique factorisation the only ideals of $\mathcal{O}_K$ containing $\mathfrak{p}^n$ are $\mathfrak{p}^l$ for $l \leq n$, so $\mathcal{O}_K/\mathfrak{p}^n$ has a unique maximal ideal $\mathfrak{p}/\mathfrak{p}^n$. So all $x \notin \mathfrak{p}/\mathfrak{p}^n$ are invertible, hence

$$\left|(\mathcal{O}_K/\mathfrak{p}^n)^\times\right| = (p^k - 1)p^{k(n-1)}.$$

$(\mathcal{O}_K/\mathfrak{p}^n)^\times$ projects onto $(\mathcal{O}_K/\mathfrak{p})^\times \cong C_{p^k-1}$, hence $(\mathcal{O}_K/\mathfrak{p}^n)^\times \cong C_{p^k-1} \times A$. $\square$

Example Let $K = \mathbb{Q}(i)$. If $\mathfrak{m} = (1)$ then $I_\mathfrak{m}/P_\mathfrak{m}^1 = 1$ as $|\mathcal{C}\ell_K| = 1$. The class field of $(\mathfrak{m}, P_\mathfrak{m}^1)$ is K itself. By Thm. 63 (iii) if F/K is an abelian extension unramified at all primes, it is a class field of $((1), H)$. Hence there are no such extensions of $\mathbb{Q}(i)$ (except for $\mathbb{Q}(i)$ itself).

Example Let $K = \mathbb{Q}(i)$. If $\mathfrak{m} = (7)$ then we have by Lemma 65:

$$I_\mathfrak{m}/P_\mathfrak{m}^1 \cong \left(\mathbb{Z}[i]/(7)\right)^\times / \{\pm 1, \pm i\} \cong C_{48}/C_4 \cong C_{12}.$$

Take $I_\mathfrak{m} \supseteq H \supseteq P_\mathfrak{m}^1$ with $I_\mathfrak{m}/H \cong C_4$. Explicitly it is given by the classes of $1, \ldots, 6, i, \ldots, 6i \in (\mathbb{Z}[i]/(7))^\times$. The class field of $(\mathfrak{m}, H)$ has $\mathrm{Gal}(F/K) \cong I_\mathfrak{m}/H \cong C_4$ and is ramified only at (7) by Thm. 63. What is F? By Kummer theory we have $F = K(\sqrt[4]{\alpha})$ for some $\alpha \in K$. Scaling by x^n, we can assume that $\alpha \in \mathcal{O}_K$ and $(\alpha) = \prod \mathfrak{p}_i^{n_i}$ with $1 \leq n_i \leq 3$. As (α) is a fourth power in F, each $\mathfrak{p}_i$ ramifies, so only $\mathfrak{p}_i = (7)$ is allowed, i. e. $\alpha = i^a 7^b$ with $0 \leq a, b \leq 3$. We further know that $b = 0, 2$ cannot occur as otherwise $K(\sqrt{\alpha})/K$ is unramifies at (7) as well. This is a contradicition to the previous example. (Note that $X^2 - \alpha$ has distinct factors modulo 7, so the inertia group is trivial.) Hence we have w. l. o. g. $b = 1$ (replace α by $\frac{1}{\alpha}7^b$), so $F = K(\sqrt[4]{\alpha})$ with $\alpha = i^a 7$. We now can either work out the ramification to find that $F = K(\sqrt[7]{-7})$ (since the other ramify at $(1 + i)$), or just compute $\mathrm{Frob}_\mathfrak{p}$, e. g. if $\mathfrak{p} = (x)$ with $x \in H$ then $\mathrm{Frob}_\mathfrak{p} = \mathrm{id}$. Take $x = 7 + 2i$ (this is a prime above $53 = (7 + 2i)(7 - 2i)$). If $\mathfrak{p} = (x)$ then $\mathrm{Frob}_\mathfrak{p} = \mathrm{id}$ as $\mathfrak{p} \in H$, so

$$\begin{aligned} \sqrt[4]{\alpha} = \mathrm{Frob}_\mathfrak{p}(\sqrt[4]{\alpha}) &\equiv \sqrt[4]{\alpha}^{53} \equiv \alpha^{13}\sqrt[4]{\alpha} \equiv (i^a 7)^1 3\sqrt[4]{\alpha} \mod \mathfrak{p} \\ &\equiv i^a(-2i)^{13}\sqrt[4]{\alpha} \equiv i^{a-i}2^{13}\sqrt[4]{\alpha} \equiv i^{a-1}30\sqrt[4]{\alpha} \equiv -i^a\sqrt[4]{\alpha} \mod \mathfrak{p}. \end{aligned}$$

(Note that $2^{13} \equiv 30 \mod 53$.) Hence $a = 2$, and so $F = K(\sqrt[4]{\alpha})$. Therefore all $\mathfrak{p} = (x)$ with $x \equiv \pm 1, \pm 2, \pm 3, \pm i, \pm 2i, \pm 3i \mod 7$ split completely in $K(\sqrt[4]{\alpha})/K$.

4.5. Ray Class Fields

25.11. **Definition** Let $\mathfrak{m}$ be a modulus of K. Its *ray class group* is $I_\mathfrak{m}/P_\mathfrak{m}^1$. Its *ray class field* $K_\mathfrak{m}$ is the class field of $(\mathfrak{m}, P_\mathfrak{m}^1)$.

Remark When $\mathfrak{m} = (1)$ the ray class group is $\mathcal{C}\ell_K$. The corresponding field $K_{(1)}$ is called the *Hilbert class field*.

Example Let $K = \mathbb{Q}$ and $\mathfrak{m} = N \cdot \infty$. Then $K_\mathfrak{m} = \mathbb{Q}(\zeta_N)$.

Lemma 66 *Let K be a number field and $\mathfrak{m}$ be a modulus.*

(i) $\mathrm{Gal}(K_\mathfrak{m}/K) \cong I_\mathfrak{m}/P^1_\mathfrak{m}$.

(ii) The class field F of $(\mathfrak{m}, H)$ lies inside $K_\mathfrak{m}$ and $\mathrm{Gal}(K_\mathfrak{m}/K) \cong H$,[1] *i. e. $F = K_\mathfrak{m}^H$.*

(iii) If $\mathfrak{m} \mid \mathfrak{m}'$ then $K_\mathfrak{m} \subseteq K_{\mathfrak{m}'}$.

Proof. (i) Follows from Thm. 63 (iv).

(ii) $K_\mathfrak{m}^H$ is a class field for $(\mathfrak{m}, H)$. (Note $\mathrm{Frob}_\mathfrak{p}(K_\mathfrak{m}^H/K) = \mathrm{id}$ iff $\mathfrak{p} \in H$ by Rmk. 58.) Hence it is *the* class field of $(\mathfrak{m}, H)$ by uniqueness (Thm. 63 (ii)).

(iii) $K_\mathfrak{m}$ is the class field for $(\mathfrak{m}', I_{\mathfrak{m}'} \cap H)$ where H is the kernel of the Artin map

$$\varphi : I_\mathfrak{m} \longrightarrow \mathrm{Gal}(K_\mathfrak{m}^H/K).$$

(Note that $H \supseteq P^1_\mathfrak{m} \supseteq P^1_{\mathfrak{m}'}$.) Hence $K_\mathfrak{m} \subseteq K_{\mathfrak{m}'}$ by (ii). □

Lemma 67 *Let K be a number field and $F = K_{(1)}$ be its Hilbert class field.*

(i) $\mathcal{C}\ell_K \cong \mathrm{Gal}(F/K)$ *(via Artin map $\prod \mathfrak{p} \to \prod \mathrm{Frob}_\mathfrak{p}$).*

(ii) A prime $\mathfrak{p}$ of K is principal iff $\mathfrak{p}$ splits completely in F/K.

(iii) The order of $\mathfrak{p}$ in $\mathcal{C}\ell_K$ is equal to the order of $\mathrm{Frob}_\mathfrak{p}$ *in* $\mathrm{Gal}(F/K)$ *and $f_\mathfrak{p}$, the residue degree of $\mathfrak{p}$ in F/K.*

(iv) F/K is unramified at all primes and all embeddings $K \hookrightarrow \mathbb{R}$ extend to $F \hookrightarrow \mathbb{R}$. If L/K is another abelian extension with this property, then $L \subseteq F$.

Proof. (i) Follows from Thm. 63 (iv).

(ii) A prime $\mathfrak{p}$ is principal iff $\mathfrak{p} \in P^1_\mathfrak{m}$ with $\mathfrak{m} = (1)$ iff $\mathrm{Frob}_\mathfrak{p} = \mathrm{id}$.

(iii) Follows by (i).

(iv) F/K satisfies this property because its conductor is (1) (by Thm. 63 (iii)). Also L has conductor (1) (by Thm. 63 (i) and (iii)), so is a class field for $((1), H)$, so lies in F (by Lemma 66 (ii)). □

Example Let $K = \mathbb{Q}\big(\sqrt{-5}\big)$, so $\mathcal{O}_K = \mathbb{Z}\big[\sqrt{-5}\big]$ and $\mathcal{C}\ell_K = C_2$. Its Hilbert class field is $F = K(i)$ since only 2 and 5 ramify in $F/\mathbb{Q}$ and the primes above these in K are unramified in F/K. Moreover K has no real embeddings. Hence $F \subseteq K_{(1)}$ by Lemma 67 (iv), and so $F = K_{(1)}$ as $\mathrm{Gal}(F/K) \cong \mathcal{C}\ell_K$ by Lemma 67 (i). Explicitly: Let $\mathfrak{p} \nmid 2$ be a prime of K. If $\mathfrak{p} = (a + b\sqrt{-5})$ then $N(\mathfrak{p}) = a^2 + 5b^2 \equiv 1 \mod 4$ since $N(\mathfrak{p})$ must be odd. So $\mathrm{Frob}_\mathfrak{p}(i) \equiv i^{N(\mathfrak{p})} \equiv i \mod \mathfrak{p}$, and hence $\mathrm{Frob}_\mathfrak{p} = \mathrm{id}$ since $i \not\equiv -i \mod \mathfrak{p}$ as $\mathfrak{p} \nmid 2$. If $\mathfrak{p}$ is non-principal then $\mathfrak{p}(3, 1 + \sqrt{-5})$ is, so $N(\mathfrak{p}) \cdot 3 = a^2 + 5b^2 \equiv 1 \mod 4$ (again $N(\mathfrak{p})$ must be odd). This implies $N(\mathfrak{p}) \equiv 3 \mod 4$, and hence $\mathrm{Frob}_\mathfrak{p}(i) \equiv i^{N(\mathfrak{p})} \equiv -i \mod \mathfrak{p}$, i. e. $\mathrm{Frob}_\mathfrak{p} \neq \mathrm{id}$ as $i \not\equiv -i \mod \mathfrak{p}$. Thus $\mathfrak{p}$ has

[1] Note the abuse of notation H for $H/P^1_\mathfrak{m}$.

residue degree 2 in F/K. Finally $\mathfrak{p} \mid 2$ is non-principal (explicitly $\mathfrak{p} = (2, 1+\sqrt{-5})$), and does not split in F/K.

Proposition 68 *Let K/k be a Galois extension of number fields and $\mathfrak{m}$ a modulus of K with $\mathfrak{m} = g\mathfrak{m}$ for all $g \in \mathrm{Gal}(K/k)$. Then:*

(i) *$K_\mathfrak{m}$ is Galois over k.*

(ii) *If $\mathfrak{n} \mid \mathfrak{m}$ then $K_{g\mathfrak{n}} = \tilde{g}K_\mathfrak{n}$ for any $\tilde{g} \in \mathrm{Gal}(K_\mathfrak{m}/k)$ that projects to $g \in \mathrm{Gal}(K/k)$.*

(iii) *$\varphi(g\mathfrak{a}) = \tilde{g}\varphi(\mathfrak{a})\tilde{g}^{-1}$, where $\varphi : I_\mathfrak{m} \to \mathrm{Gal}(K_\mathfrak{m}/K)$ is the Artin map and g, $\tilde{g}$ as in (ii).*

Proof. Let F/k be the Galois closure of $K_\mathfrak{m}/k$, and $\mathfrak{q}$ a prime of F above $\mathfrak{p}$. Observe that

$$\sigma \operatorname{Frob}_{\mathfrak{q}/\mathfrak{p}} \sigma^{-1} = \operatorname{Frob}_{\sigma(\mathfrak{q})/\sigma(\mathfrak{p})} \tag{4.1}$$

for $\sigma \in \mathrm{Gal}(F/k)$.

(i) $\mathfrak{p}$ splits completely in $\sigma K_\mathfrak{m}$ iff $\sigma^{-1}\mathfrak{p}$ splits completely in $K_\mathfrak{m}$ iff $\mathfrak{p}$ splits completely in $K_\mathfrak{m}$ as the definition of $K_\mathfrak{m}$ is $\mathrm{Gal}(F/k)$-invariant. Thus $\sigma K_\mathfrak{m}$ is also a class field for $\mathfrak{m}$ and so $\sigma K_\mathfrak{m} = K_\mathfrak{m}$ by uniqueness. Hence $K_\mathfrak{m}/k$ is Galois.

(ii) $\mathfrak{p}$ splits completely in $\sigma K_\mathfrak{n}$ iff $\operatorname{Frob}_{\mathfrak{q}/\mathfrak{p}} \in \mathrm{Gal}(F/K_\mathfrak{n})$ iff $\sigma \operatorname{Frob}_{\mathfrak{q}/\mathfrak{p}} \sigma^{-1} \in \mathrm{Gal}(F/\sigma K_\mathfrak{n})$ iff $\operatorname{Frob}_{\sigma(\mathfrak{q})/\sigma(\mathfrak{p})} \in \mathrm{Gal}(F/\sigma K_\mathfrak{n})$ iff $\sigma(\mathfrak{p})$ splits completely in $\sigma K_\mathfrak{n}$. Hence $\sigma K_\mathfrak{n}$ is a class field for $\sigma\mathfrak{n}$ and so $\sigma K_\mathfrak{n} = K_{\sigma\mathfrak{n}}$.

(iii) Follows by (4.1). □

Remark For the Hilbert class field we have: $\mathfrak{p}$ is principal iff $\mathfrak{p}$ splits completely. For $\mathfrak{p}$ non-principal Hilbert conjectured that $\mathfrak{p}\mathcal{O}_F$ is principal, which turned out to be true.

4.6. Properties of the Artin Map*

27.11. **Definition** Let F/K be a Galois extension and K^{ab} the maximal abelian extension of K in F, so if $\mathrm{Gal}(F/K) = G$ then $\mathrm{Gal}(F/K^{\mathrm{ab}}) = G'$ and $\mathrm{Gal}(K^{\mathrm{ab}}/K) = G/G'$, where $G' = \langle aba^{-1}b^{-1} : a, b \in G\rangle$ is the commutator subgroup. The *Artin mapArtin map* is defined by

$$\varphi_{F/K} : I_\mathfrak{m} \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K) = G/G', \qquad \mathfrak{p} \longmapsto \operatorname{Frob}_\mathfrak{p} G'.$$

Remark If L/K finite, then

$$H = \mathrm{Gal}(FL/L) \leq \mathrm{Gal}(F/K) = G.$$

(Any automorphism of FL/K restricts to an automorphism of F/K; if it acts trivially on F and on L, then it acts trivially on FL.) There's a natural map

$$H/H' \longrightarrow G/G', \qquad hH' \longrightarrow hG'$$

induced by this inclusion.

Definition Let F/K be a Galois extension of number fields and $G = \mathrm{Gal}(F/K)$. The *relative norm* of an ideal $\mathfrak{a} \lhd \mathcal{O}_F$ is an ideal $N_{F/K}(\mathfrak{a}) \lhd \mathcal{O}_K$ with

$$N_{F/K}(\mathfrak{a})\mathcal{O}_F = \prod_{g \in G} g(\mathfrak{a}).$$

Remark (*i*) $N_{F/K}((\alpha)) = (N_{F/K}(\alpha))$.

(*ii*) If $\mathfrak{q}$ lies above $\mathfrak{p}$, then

$$\prod_{g \in G} g(\mathfrak{q}) = (\mathfrak{q}_1 \cdots \mathfrak{q}_k)^{ef},$$

where $\mathfrak{q}_i$ are the primes are the primes above $\mathfrak{p}$. So $N_{F/K}(\mathfrak{q}) = \mathfrak{p}^{f_\mathfrak{q}}$, where $f_\mathfrak{q}$ is the residue degree.

Lemma 69 (*) *Let F and L be Galois extensions of K, with FL/L abelian, and $\mathfrak{m}$ a suitable modulus (i. e. the conorm of the conductor of K^{ab}/K). Then*

$$\varphi_{F/K}(N_{L/K}(\mathfrak{a})) = \varphi_{FL/L}(\mathfrak{a}) \cdot G',$$

for $(\mathfrak{a}, \mathfrak{m}) = 1$. *Equivalently, the following commutes:*

$$\begin{tikzcd} I_\mathfrak{m} \arrow[r, "\varphi_{F/K}"] \arrow[d, "N_{L/K}"'] & H \arrow[d] \\ I_{N(\mathfrak{m})} \arrow[r, "\varphi_{FL/K}"'] & G/G' \end{tikzcd}$$

Proof. It is enough to check the statement on primes as $N_{L/K}$ is multiplicative. Let $\mathfrak{q}$ be a prime of L above $\mathfrak{p}$ (where $\mathfrak{p}$ is unramified in F/K). Then:

$$\varphi_{F/K}(N_{L/K}(\mathfrak{q})) = \varphi(\mathfrak{p}^{f_\mathfrak{p}}) = \mathrm{Frob}_\mathfrak{p}^{f_\mathfrak{p}}(F/K) = \mathrm{Frob}_\mathfrak{q}(FL/L) = \varphi(\mathfrak{q}). \qquad \square$$

Corollary 70 (*) *Suppose F/K is abelian. If $\mathfrak{p} = N_{F/K}(\mathfrak{q})$, then* $\mathrm{Frob}_\mathfrak{p} = \mathrm{id}$, *for $\mathfrak{p}$ unramified in F/K.*

Proof.

$$\mathrm{Frob}_\mathfrak{p} = \varphi_{F/K}(\mathfrak{p}) = \varphi_{F/F}(\mathfrak{q}) = \mathrm{id}\,. \qquad \square$$

Definition Let $H \le G$ be finite groups. The *transfer map* (or *Verlagerung*) $\mathrm{Ver} : G/G' \to H/H'$ is defined as follows: Let $H_{r_1}, \ldots, H_{r_k}$ be the right cosets of H in G. If $g \in G$, let $H_{r_i g} = H_{r_{\sigma(i)}}$. Then

$$\mathrm{Ver}(g) = \prod_i r_i g r_{\sigma(i)}^{-1} \cdot H'.$$

Fact: Ver is a well-defined homomorphism.

Remark We have

$$\mathrm{Ver}(g) = r_1 g r_{\sigma(1)}^{-1} \left(r_{\sigma(1)} g r_{\sigma^2(1)}^{-1} \right) \left(r_{\sigma^2(1)} g r_{\sigma^3(1)}^{-1} \right) \cdots = \prod_{s \in \Sigma} s g^{f(s)} s^{-1},$$

where $Hs\langle g\rangle$ are the $H\backslash G/\langle g\rangle$ double cosets, equivalently the $\langle g\rangle$-orbits on the H_{r_i}, and $f(s) = |Hs\langle g\rangle|/|H|$ is the length of the orbit of Hs.

Lemma 71 (*) *Let F/K be a Galois extension of number fields, L/K finite and $\mathfrak{m}$ the conductor of the maximal abelian extension of K in F. Then*

$$\varphi_{FL/L}(\mathfrak{a}\mathcal{O}_L) = \operatorname{Ver}\varphi_{F/K}(\mathfrak{a})$$

for $(\mathfrak{a},\mathfrak{m}) = 1$, i. e. the following commutes:

$$\begin{tikzcd} I_{\mathfrak{m}} \arrow[r, "\varphi_{F/K}"] \arrow[d, "conorm"'] & G/G' \arrow[d, "\mathrm{Ver}"] \\ I_{\mathfrak{m}\mathcal{O}_L} \arrow[r, "\varphi_{FL/L}"'] & H/H' \end{tikzcd}$$

Proof. It is enough to check this on the primes $\mathfrak{p}$ of K. With notation as in the remark above and $g = \mathrm{Frob}_{\mathfrak{p}}$, we have

$$\begin{aligned} \operatorname{Ver}\varphi_{F/K}(\mathfrak{p}) = \operatorname{Ver}\mathrm{Frob}_{\mathfrak{p}} = \prod_{s\in\Sigma} s\,\mathrm{Frob}_{\mathfrak{p}}^{f(s)}\,s^{-1} &\overset{\text{C30, P31}}{=} \prod_{\mathfrak{q}|\mathfrak{p}} \mathrm{Frob}_{\mathfrak{q}} \\ = \prod_{\mathfrak{q}|\mathfrak{p}} \varphi_{FL/L}(\mathfrak{q}) = \varphi_{FL/L}(\mathfrak{p}\mathcal{O}_L), \end{aligned}$$

as $\mathfrak{p}$ is unramified. □

Theorem 72 (Furtwängler*) *Let G be a finite group and $H = G'$. The transfer map* Ver *from G to H is trivial, i. e.* $\operatorname{Ver}(\mathfrak{q}) = \mathrm{id}$.

Proof. Hard! □

Corollary 73 (Principal Ideal Theorem*) *All ideals in a number field K become principal in its Hilbert class field, i. e. $\mathfrak{a}\mathcal{O}_{K_{(1)}} = (\alpha)$ for some $\alpha \in \mathcal{O}_{K_{(1)}}$.*

Proof. Let $F = K_{(1)}$. By Prop. 68, $F_{(1)}$ is Galois over K. Let $G = \mathrm{Gal}(F_{(1)}/K)$ and $H = \mathrm{Gal}(F_{(1)}/F)$. Note that all subfields L of $F_{(1)}$ are unramified at all primes of K, and all $K \hookrightarrow \mathbb{R}$ extend to $L \hookrightarrow \mathbb{R}$. As $F = K_{(1)}$ is the maximal abelian such field we have $H = G'$. If $\mathfrak{p}$ is a prime of K, we have

$$\varphi_{F_{(1)}/F}(\mathfrak{p}\mathcal{O}_F) \overset{\text{L71}}{=} \mathrm{Ver}_{G\to H}(\mathrm{Frob}_{\mathfrak{p}}) \overset{\text{T72}}{=} \mathrm{id}\,.$$

Thus $\mathfrak{p}\mathcal{O}_F$ is principal by Lemma 67 (ii). So all ideals become principal in $\mathcal{O}_F$. □

A. Appendix: Local Fields*

A.1. Definitions

Definition A *place* in a number field K is an equivalence class of (non-trivial) absolute values on K. 30.11.

Remark These places come in two flavours:

- The *infinite places* (corresponding to the *archimedian absolute values*) come from embeddings $K \hookrightarrow \mathbb{R}$ or $K \hookrightarrow \mathbb{C}$ and taking

$$|x|_{\mathrm{v}} = \begin{cases} |x|, & \text{for real embeddings,} \\ |x|^2, & \text{for complex embeddings.} \end{cases}$$

  Note: Complex conjugate embeddings give the same $|x|_{\mathrm{v}}$. *Fact*: Each archimedian absolute value arises in this way, whereas the rest does not, thus the number of infinite places is $r_1 + r_2$.

- The finite places (corresponding to the non-archimedian absolute values) correspond to the primes in K: If $\mathfrak{p}$ is a prime, set $|x|_{\mathfrak{p}} = N(\mathfrak{p})^{-\operatorname{ord}_{\mathfrak{p}}(x)}$, where $\operatorname{ord}_{\mathfrak{p}}(x)$ for $x \in \mathcal{O}_K$ is the power of $\mathfrak{p}$ in the factorisation of (x) and extended multiplicatively to K. *Fact*: These are inequivalent (for different $\mathfrak{p}$) and there are no others.

Remark *Completions*: The absolute value $|\cdot|_{\mathrm{v}}$ makes K into a metric space. Its completion K_{v} is a complete local field. If v is archimedian then K_{v} is $\mathbb{R}$ or $\mathbb{C}$. (These are the "boring" extensions.) Henceforth assume v is a finite place. If $K = \mathbb{Q}$ and v corresonds to p, then $K_{\mathrm{v}} = \mathbb{Q}_p$. If K is general, v corresonds to $\mathfrak{q}$, where $\mathfrak{q}$ lies above p. Then $|\cdot|_{\mathrm{v}}$ on $\mathbb{Q}$ is equivalent to $|\cdot|_p$. Thus K_{v} is a finite extension of $\mathbb{Q}_p$.

A.2. Residue Fields and Ramification

Remark (*i*) Let K be a number field and v an absolute value corresponding to $\mathfrak{q}$. Then $\mathcal{O}_{K_{\mathrm{v}}} \subseteq K_{\mathrm{v}}$ are the elements with $|x|_{\mathrm{v}} \leq 1$, the units $\mathcal{O}_{K_{\mathrm{v}}}^{\times}$ are the elements with $|x|_{\mathrm{v}} = 1$, the (unique) maximal ideal $\mathfrak{m}_{\mathrm{v}}$ of $\mathcal{O}_{K_{\mathrm{v}}}$ are the elements with $|x|_{\mathrm{v}} < 1$, and the associate residue field is $k_{\mathrm{v}} = \mathcal{O}_{K_{\mathrm{v}}}/\mathfrak{m}_{\mathrm{v}}$.

(*ii*) Observe that $\mathcal{O}_K \subseteq \mathcal{O}_{K_{\mathrm{v}}}$ and $\mathfrak{q} \subseteq \mathfrak{m}_{\mathrm{v}}$. So the mapping

$$\mathcal{O}_K/\mathfrak{q} \longrightarrow \mathcal{O}_{K_{\mathrm{v}}}/\mathfrak{m}_{\mathrm{v}}$$

is both injective (clear as it is a field homomorphism) and surjective (every element of K_{v} can be approximated by an element of K). Hence $\mathcal{O}_K/\mathfrak{q} = k_{\mathrm{v}}$, so the residue field does not change by completing.

(*iii*) If L/K is a finite extension and $\mathfrak{r}$ is a prime of L above $\mathfrak{q}$, then $L_{\mathrm{w}}/K_{\mathrm{v}}$ is finite, $f_{\mathfrak{r}/\mathfrak{q}} = f_{\mathrm{w}\,/\,\mathrm{v}}$ (by above), and $e_{\mathfrak{r}/\mathfrak{q}} = e_{\mathrm{w}\,/\,\mathrm{v}}$ (by comparing valuations).

A.3. Galois Groups

Lemma *Let F/K be a Galois extension of number fields and $\mathfrak{q}$ a prime of F above $\mathfrak{p}$ with corresponding absolute values* w *and* v*, respectively. If $g \in D_{\mathfrak{q}/\mathfrak{p}}$ then it preserves $|\cdot|_{\mathrm{w}}$ on F, so it is a topological isomorphism and thus it extends to an automorphism of F_{w}. Hence we obtain a mapping*

$$D_{\mathfrak{q}/\mathfrak{p}} \longrightarrow \mathrm{Gal}(F_{\mathrm{w}}/K_{\mathrm{v}}).$$

Proposition *This is an isomorphism.*

Proof. It is clear that the mapping is injective. For surjectivity we have

$$|D_{\mathfrak{q}/\mathfrak{p}}| = e_{\mathfrak{q}/\mathfrak{p}} \cdot f_{\mathfrak{q}/\mathfrak{p}} = e_{\mathrm{w}\,/\,\mathrm{v}} \cdot f_{\mathrm{w}\,/\,\mathrm{v}} = [F_{\mathrm{w}} : K_{\mathrm{v}}] = |\,\mathrm{Gal}(F_{\mathrm{w}\,/\,\mathrm{v}})|.$$

Observe also that we have $I_{\mathfrak{q}/\mathfrak{p}} \xrightarrow{\sim} I_{\mathrm{w}\,/\,\mathrm{v}}$ (being the element that acts trivially on respective residue fields). □

A.4. Applications

Proposition (cf. Prop. 22) *If $f \in \mathcal{O}_K[X]$ is Eisenstein with respect to $\mathfrak{p}$ and α is a root, then $K(\alpha)/K$ has degree* $\deg f$ *and is totally ramified at $\mathfrak{p}$.*

Proof. Follows from the corresponding result on the completions. □

Proposition *Decomposition groups are soluble.*

Proof. Galois groups of finite extensions of $\mathbb{Q}_p$ are $I \lhd G$ with G/I cyclic and $I_1 \lhd I$ with I/I_1 cyclic, where I_1 is a p-group. □

Example There are no C_4-extensions of $\mathbb{Q}$ whose quadratic subfield is $\mathbb{Q}(\zeta_3)$.

Proof. The extension $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ is ramified at 3, so the inertia at 3 must be all of C_4. It is complete at 3 since if you get $F_{\mathrm{w}}/\mathbb{Q}_3$ totally ramified and cyclic of degree 4, this is a tame extension of $\mathbb{Q}_3$, so

$$\mathrm{Gal}(F_{\mathrm{w}}/\mathbb{Q}_3) \hookrightarrow \mathbb{F}_3^\times,$$

which is a contradiction. □

As an outlook, there is local class field theory, local reciprocity, and much more.

Section A

1 Give the definition of a Dedekind domain. Let $\mathfrak{o}$ be a Dedekind domain with field of fractions k. Let $\mathfrak{a}$ be a non-zero fractional ideal in k and define $\mathfrak{a}^{-1} = \{ x \in k \mid x\mathfrak{a} \subset \mathfrak{o} \}$. Show that $\mathfrak{a}^{-1}$ is a fractional ideal and that $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{o}$.

2 (i) State and prove the Chinese remainder theorem for $\mathfrak{o}$ a Dedekind domain.

(ii) Let K/k be a normal extension of algebraic number fields. Let $\mathfrak{p}$ be a prime of k, whose factorisation in K is $\operatorname{conorm}_{K/k} \mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$. Show that $\mathrm{Gal}(K/k)$ acts transitively on the $\mathfrak{P}_i$.

3 Let K/k be a finite extension of algebraic number fields. Define the relative ideal norm and prove that it is multiplicative. Let $\mathfrak{p}$ be a prime of k, whose factorisation in K is $\operatorname{conorm}_{K/k} \mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$. Show that $[K : k] = \sum e_i f_i$ where f_i is the degree of $\mathfrak{O}/\mathfrak{P}_i$ over $\mathfrak{o}/\mathfrak{p}$.

[*Properties of the norm for elements may be assumed.*]

Section B

4 Let K/k be an extension of algebraic number fields. Let $\mathfrak{p}$ be a prime of k and $\mathfrak{P}$ a prime of K above $\mathfrak{p}$.

(i) Let $f(X)$ be a monic polynomial in $\mathfrak{o}_\mathfrak{p}[X]$ and suppose that the reduction mod $\mathfrak{p}$ factors as $\tilde{f}(X) = \phi_1(X)\phi_2(X)$ where ϕ_1, ϕ_2 in $(\mathfrak{o}/\mathfrak{p})[X]$ are coprime. Show that $f(X) = f_1(X) f_2(X)$ with $\tilde{f_\nu}(X) = \phi_\nu(X)$.

(ii) Suppose $\mathfrak{P}^e \mid\mid \mathfrak{p}$ and $\mathfrak{p} \mid e$. Show that if $\alpha \in \mathfrak{O}_\mathfrak{P}$ then $\mathrm{Tr}_{K_\mathfrak{P}/k_\mathfrak{p}}(\alpha) \in \mathfrak{p}_\mathfrak{p}$.

5 Let K/k be an extension of algebraic number fields. Define the relative different $\mathfrak{d}_{K/k}$. In the case $k = \mathbf{Q}$ describe the relationship with the discriminant d_K.

(i) For $K \supset L \supset k$ show that $\mathfrak{d}_{K/k} = \mathfrak{d}_{K/L}\mathfrak{d}_{L/k}$.

(ii) State a relationship between the different and ramification. Hence show that if K_1, K_2 are Galois over $\mathbf{Q}$ with coprime discriminants, then $[K_1K_2 : \mathbf{Q}] = [K_1 : \mathbf{Q}][K_2 : \mathbf{Q}]$.

Section C

6

Write an essay on the Hilbert class field. Illustrate by computing the Hilbert class field for *either* $\mathbf{Q}(\sqrt{-23})$ *or* $\mathbf{Q}(\sqrt{-30})$, explaining all necessary working.

[*The cubic* $X^3 + aX + b$ *has discriminant* $-4a^3 - 27b^2$.]

7 Let $m = m_1 m_2^2$ with m_1, m_2 coprime square-free positive integers. Suppose $m_1 \not\equiv \pm m_2 \pmod 9$. Show that $\mathbf{Q}(\sqrt[3]{m})$ has discriminant $-27m_1^2 m_2^2$. Find a unit in $\mathbf{Q}(\sqrt[3]{6})$ and show that this field has class number $h = 1$.

8 Let K/k be a quadratic extension of algebraic number fields with K totally complex and k totally real.

(i) Show that $[\mathfrak{O}_K^* : \mathfrak{o}_k^* \mu_K] = 1$ or 2, where $\mathfrak{O}_K^*$, $\mathfrak{o}_k^*$ are the unit groups in K, k, and μ_K is the group of roots of unity in K.

(ii) Show that the class number of k divides the class number of K.

[*You may assume any properties of the Hilbert class field you require.*]

ζ_n denotes a primitive n^{th} root of unity. O_K denotes the ring of integers of K.

1

(i) State the Kummer-Dedekind theorem.

(ii) Let $L = \mathbb{Q}(\alpha)$, where α is a root of the monic irreducible polynomial $f(X) \in \mathbb{Z}[X]$. Suppose p is a prime number such that $f(X)$ mod p has no repeated roots in the algebraic closure of $\mathbb{F}_p$. Prove that the index $[O_L : \mathbb{Z}[\alpha]]$ is coprime to p.

(iii) Determine which primes ramify in $\mathbb{Q}(\sqrt[11]{44})/\mathbb{Q}$. Justify your answer.

2

(i) Let F/K be a Galois extension of number fields and $\mathbf{p}$ a prime of K. Prove that the Galois group $\mathrm{Gal}(F/K)$ acts transitively on the set of primes of F above $\mathbf{p}$. Explain briefly how this may be used to determine the number of primes above $\mathbf{p}$ in an intermediate extension $K \subset L \subset F$, in terms of the decomposition group of a prime above $\mathbf{p}$ in F/K.

(ii) Let $F = \mathbb{Q}(\zeta_5, \sqrt[5]{\lambda})$ for some prime number λ. Let $\mathbf{q}$ be a prime of F above a prime p of $\mathbb{Q}$, whose decomposition group in $\mathrm{Gal}(F/\mathbb{Q})$ is cyclic of order 2. Show that there are three primes above p in $\mathbb{Q}(\sqrt[5]{\lambda})$, and two primes above p in $\mathbb{Q}(\zeta_5)$.

3 Define the Dirichlet L-function $L_N(\psi, s)$ for a Dirichlet character ψ modulo N, and state its expression as an Euler product. Prove that if ψ is non-trivial, then $L_N(\psi, s)$ is analytic on $\mathrm{Re}(s) > 0$ and that $L_N(\psi, 1) \neq 0$.

Prove Dirichlet's theorem on primes in arithmetic progressions. You may assume that for a Dirichlet character ψ,

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

converges absolutely on $\mathrm{Re}(s) > 1$ to an analytic branch of the logarithm of $L_N(\psi, s)$.

(*Standard results on convergence of Dirichlet series may be used without proof. You may also assume that the Riemann ζ-function has an analytic continuation to $\mathbb{C}$ except for a simple pole at $s = 1$.*)

4

Let $F = \mathbb{Q}(\zeta_3, \sqrt[3]{3})$, and let ρ be the two-dimensional irreducible representation of $\mathrm{Gal}(F/\mathbb{Q}) \simeq S_3$. Compute the first ten coefficients $a_1, \ldots, a_{10}$ of its Artin L-series $L(\rho, s) = \sum_n a_n\, n^{-s}$.

END OF PAPER

1

State and prove the Kummer–Dedekind theorem. Determine which primes ramify in $\mathbb{Q}(\zeta_{80})/\mathbb{Q}$, where ζ_n denotes a primitive n-th root of 1.

[*You may assume that the ring of integers of* $\mathbb{Q}(\zeta_n)$ *is* $\mathbb{Z}[\zeta_n]$.]

2

(i) Let F/K be a Galois extension of number fields. Let $\mathfrak{p}$ be a prime of K with residue field $k_{\mathfrak{p}}$, and $\mathfrak{q}$ a prime of F above $\mathfrak{p}$ with residue field $k_{\mathfrak{q}}$. Prove that the natural map from the decomposition group of $\mathfrak{q}$ to $\mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$ is surjective.

Now let $F = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$, where ζ_3 denotes a primitive cube root of 1.

(ii) Prove that no prime of F has absolute residue degree 6.

(ii) The prime 7 decomposes in $\mathbb{Q}(\zeta_3)$ as $\mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1 = (\zeta_3 + 3)$ and $\mathfrak{p}_2 = (\zeta_3^2 + 3)$. Determine the Frobenius element of $\mathfrak{p}_1$ in $F/\mathbb{Q}(\zeta_3)$.

3

Let $F = \mathbb{Q}(\sqrt{-2}, \sqrt{-3})$, and let ρ be the regular representation of $\mathrm{Gal}(F/\mathbb{Q}) \simeq C_2 \times C_2$, *i.e.* the direct sum of its four 1-dimensional representations. Compute the first ten coefficients $a_1, \ldots, a_{10}$ of its Artin L-series $L(\rho, s) = \sum_{n \geqslant 1} a_n n^{-s}$.

4

State and prove Chebotarev's density theorem. Prove that for a monic irreducible polynomial $f(X)$ with integer coefficients, there are infinitely many primes p such that $f(X) \mod p$ has no roots in $\mathbb{F}_p$.

[*You may assume that Artin* L*-functions have meromorphic continuation to* $\mathbb{C}$*, analytic on* $\Re(s) > 1$*, that the Riemann* ζ*-function* $\zeta(s)$ *has a simple pole at* $s = 1$*, and that* $L(\rho, s)$ *is analytic and non-zero at* $s = 1$ *for non-trivial irreducible representations* ρ.]

END OF PAPER

Bibliography

[Cas86] John William Scott Cassels, *Local fields*, Cambridge University Press, Cambridge, 1986.

[Cox89] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, Wiley, New York, 1989.

[Hec23] Erich Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Akademische Verlagsgesellschaft, Leipzig, 1923.

[Hec81] ______, *Lectures on the theory of algebraic numbers*, Springer, New York, 1981.

[IR90] Kenneth F. Ireland and Michael I. Rosen, *A classical introduction to modern number theory*, 2 ed., Springer, Berlin, 1990.

[Jan96] Gerald J. Janusz, *Algebraic number fields*, 2 ed., American Mathematical Society, Providence, 1996.

[Kob84] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, 2 ed., Springer, New York, 1984.

[Lan94] Serge Lang, *Algebraic number theory*, 2 ed., Springer, New York, 1994.

[Lem00] Franz Lemmermeyer, *Reciprocity laws : from euler to eisenstein*, Springer, Berlin, 2000.

[MSP06] Stefan Müller-Stach and Jens Piontkowski, *Elementare und algebraische Zahlentheorie. Ein moderner Zugang zu klassischen Themen*, Vieweg, Wiesbaden, 2006.

[Neu07] Jürgen Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin, 2007.

[Sch07] Alexander Schmidt, *Einführung in die algebraische Zahlentheorie*, Springer, Berlin, 2007.

[SD01] H. P. F. Swinnerton-Dyer, *A brief guide to algebraic number theory*, Cambridge University Press, Cambridge, 2001.

[Ser73] Jean-Pierre Serre, *A course in arithmetic*, Springer, New York, 1973.

[Ser79] ______, *Local fields*, Springer, New York / London, 1979.

[Zag81] Don B. Zagier, *Zetafunktionen und quadratische Körper: Eine Einführung in die höhere Zahlentheorie*, Springer, Berlin, 1981.

Index