Algebraic Number Theory

Dr V. Dokchitser (V.Dokchitser@dpmms.cam.ac.uk)
Typeset by Aaron Chan (akyc2@cam.ac.uk)

Last update: July 19, 2010

1 Number Fields

1.1 Ring of integers

Definition 1.1
A number field K is a finite field extension of $\mathbb{Q}$. (Its degree $[K:\mathbb{Q}] = \dim_{\mathbb{Q}} K$ as vector space is finite)

Definition 1.2
An algebraic integer α is an algebraic number s.t. it is a root of a monic polynomial with integer coefficient.
(Equivalently, if the monic minimal polynomial for α over $\mathbb{Q}$ has $\mathbb{Z}$ coefficient)

Definition 1.3
Let K be a number field, its ring of integers $\mathcal{O}_K$ consists of the element of K that are algebraic integers.

Proposition 1.4
(i) $\mathcal{O}_K$ is a (Noetherian) ring
(ii) $\mathrm{rk}_{\mathbb{Z}}\, \mathcal{O}_K = [K:\mathbb{Q}]$ (i.e. as an abelian group, $\mathcal{O}_K \cong \mathbb{Z}^{\oplus [K:\mathbb{Q}]}$)
(iii) $\forall \alpha \in K, \exists n \in \mathbb{Z}, n \neq 0$ s.t. $n\alpha \in \mathcal{O}_K$

Example:

Number Fields K	Ring of integers $\mathcal{O}_K$
$\mathbb{Q}$	$\mathbb{Z}$
$\mathbb{Q}(i)$	$\mathbb{Z}[i]$
$\mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}\setminus\{0\}$ squarefree	$\begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2,3 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \mod 4 \end{cases}$
$\mathbb{Q}(\zeta_n)$ (ζ_n primitive n-th root of 1)	$\mathbb{Z}[\zeta_n]$

Example:
$K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3) \qquad \mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \mathbb{Z}[\zeta_3] \quad (\zeta_3 = \frac{-1-\sqrt{-3}}{2})$ (see notes for picture)

Proposition 1.5
(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 $f \in \mathcal{O}_K[x]$ monic and $f(\alpha) = 0 \quad \alpha \in K$, then $\alpha \in \mathcal{O}_K$)

Example (on factorisations)
In $\mathbb{Z}$, however you factorise an integer, you always end up with the same factorisation into irreducible bits, at least up to signs and order.
-The ambiguity in signs comes from the units $\pm 1 \in \mathbb{Z}$
-Unique factorisation in this form fails in general number field
e.g. $\mathbb{Q}[\sqrt{-5}]$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$
$6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ are genueinly different factorisations (because $\mathbb{Z}[\sqrt{-5}]$ not UFD).
To rescue this, works with ideals.

1.2 Units

Definition 1.6
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 unit is denote by $\mathcal{O}_K^\times$

Example: Units in $\mathbb{Q}$ are $\mathbb{Z}^\times = \{\pm 1\}$
Units in $\mathbb{Q}(i)$ are $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$
Units in $\mathbb{Q}(\sqrt{2})$ are $\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}$

Theorem 1.7 (Dirichlet's Unit Theorem)
Let K be a number field, then $\mathcal{O}_K$ is finitely generated. More precisely,

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

where

$$\begin{aligned}
\Delta &= \text{the (finite) group of roots of unity in } K \\
r_1 &= \#\text{ distinct embedding } K \hookrightarrow \mathbb{R} \\
r_2 &= \#\text{ distinct conjugate pairs of embedding } K \hookrightarrow \mathbb{C}\text{, with image } \not\subseteq \mathbb{R} \\
& (\Rightarrow r_1 + 2r_2 = [K:\mathbb{Q}])
\end{aligned}$$

Corollary 1.8
The only number fields with finitely many non-units are $\mathbb{Q}$, and imaginary quadratic fields (i.e. $\mathbb{Q}(\sqrt{-D})$ for some $D \in \mathbb{Z}^+$)

1.3 Ideals

Example 1.9 (i) $K = \mathbb{Q}$ $\quad \mathcal{O}_K = \mathbb{Z}$
$\mathfrak{a} = (17)$=all multiples of 17
$\alpha \in \mathfrak{a}$ iff it is a multiple of 17
Multiplying ideals: $(3)(17) = (51)$

(ii) $K = \mathbb{Q}(\sqrt{-5})$ $\quad \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ (not PID) (see picture)

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

Theorem 1.10 (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 1.11
Let $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_K$. Then $\mathfrak{a}$ divides $\mathfrak{b}$ (written $\mathfrak{a}\,|\,\mathfrak{b}$) if $\mathfrak{a}\,\mathfrak{c} = \mathfrak{b}$ for some ideal $\mathfrak{c}$ (Equivalently if the prime factorisations $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}, \quad \mathfrak{b} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_k^{m_k}$ we have $n_i \leq m_i\ \forall i$)

Remark. (i) For $\alpha, \beta \in \mathcal{O}_K, \quad (\alpha) = (\beta) \quad \Leftrightarrow \quad \alpha = u\beta$ for some $u \in \mathcal{O}_K^\times$

(ii) (nontrivial) For ideals $\mathfrak{a}, \mathfrak{b} \quad \mathfrak{a}\,|\,\mathfrak{b} \Leftrightarrow \mathfrak{a} \supseteq \mathfrak{b}$

(iii) To multiply ideals, simply multiply their generators
e.g. $(2)(3) = (6)$
$(2, 1+\sqrt{-5})(2, 1-\sqrt{5}) = (4, 2+2\sqrt{-5}, 2-2\sqrt{-5}, 6) = (2)$

(iv) To add ideals, combine their generators
e.g. $(2) + (3) = (2,3) = (1) = \mathcal{O}_K$

Lemma 1.12
$\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_K,\ \mathfrak{a} = \prod_i \mathfrak{p}_i^{n_i} \quad \mathfrak{b} = \prod_i \mathfrak{p}_i^{m_i}$

(i) $\mathfrak{a} \cap \mathfrak{b} = \prod_i \mathfrak{p}_i^{\max(n_i, m_i)}$ ("lcm")

(ii) $\mathfrak{a} + \mathfrak{b} = \prod_i \mathfrak{p}_i^{\min(n_i, m_i)}$ ("gcd")

Proof
Use Remark (ii)

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

(ii) This is the smallest ideal containing both $\mathfrak{a}$ and $\mathfrak{b}$

□

Lemma 1.13
Let $\alpha \in \mathcal{O}_K \setminus \{0\}$ Then $\exists \beta \in \mathcal{O}_K \setminus \{0\}$ s.t. $\alpha\beta \in \mathbb{Z} \setminus \{0\}$

Proof
Let $X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ be the minimal polynomial for α (with $a_i \in \mathbb{Z} \quad a_0 \neq 0$)
So $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha = -a_0 \in \mathbb{Z} \setminus \{0\}$
So take $\beta = \alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1$ □

Corollary 1.14
If $\mathfrak{a} \trianglelefteq \mathcal{O}_K$ is a nonzero ideal, then $[\mathcal{O}_K : \mathfrak{a}] < \infty$

Proof
Pick $\alpha \in \mathfrak{a} \setminus \{0\}$, and $\beta \in \mathcal{O}_K \setminus \{0\}$ with $N = \alpha\beta \in \mathbb{Z} \setminus \{0\}$. Then $N \in \mathfrak{a}$ and
$[\mathcal{O}_K : \mathfrak{a}] \leq [\mathcal{O}_K : (N)] = [\mathcal{O}_K : N\,\mathcal{O}_K] = |N|^{[K:\mathbb{Q}]} < \infty$ □

Definition 1.15
The <u>norm</u> of nonzero ideal $\mathfrak{a} \trianglelefteq \mathcal{O}_K$ is $N(a) = [\mathcal{O}_K : \mathfrak{a}]$

Lemma 1.16
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 linear map $T_\alpha(v) = \alpha v$
Then

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

$\square$

1.4 Ideal Class Group

K a number field. Define an equivalence relation on nonzero ideals of $\mathcal{O}_K$ by

$$\mathfrak{g} \sim \mathfrak{h} \text{ if } \exists \lambda \in K^\times s.t. \, \mathfrak{a} = \lambda \, \mathfrak{b} \tag{1.1}$$

The ideal class group of K, Cl_K, is the set of classes, {non-zero ideals}/ $\sim$
It is a group, the group structure coming from multiplication of ideals.
The principal ideals form the identity class, and $\mathcal{O}_K$ is UFD $\Leftrightarrow \mathrm{Cl}_K = 1$

Theorem 1.17
Cl_K is finite

Exercise: Let $K = \mathbb{Q}(\sqrt{-D})$ for $D \in \mathbb{Z}_+$, show that two non-zero ideals $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_K$ have the same class in Cl_K iff they are homothetic (i.e. the lattices in $\mathbb{C}$ given by the points of $\mathfrak{a}$ and $\mathfrak{b}$ are related by a scaling and a rotation about 0) (elements of $\mathrm{Cl}_K \leftrightarrow$ shapes of lattices)

1.5 Primes and Modular Arithmetic

Definition 1.18
A prime $\mathfrak{p}$ of a number field K is a nonzero prime ideal of $\mathcal{O}_K$. Its residue field is $\mathcal{O}_K \,/\, \mathfrak{p}$
Its (absolute) residue degree is $f_p = [\mathcal{O}_K \,/\, \mathfrak{p} : \mathbb{F}_p]$ where $p = \operatorname{char} \mathcal{O}_K \,/\, \mathfrak{p}$ is its residue characteristic

Lemma 1.19
The residue field of a prime is a finite field

Proof
$\mathfrak{p}$ prime $\Rightarrow$ $\mathcal{O}_K \,/\, \mathfrak{p}$ is an integral domain.
Also, $|\, \mathcal{O}_K \,/\, \mathfrak{p} \,| = N(\mathfrak{p})$ is finite $\Rightarrow$ $\mathcal{O}_K \,/\, \mathfrak{p}$ is a field $\square$

Note: The size of the residue field at $\mathfrak{p}$ is $N(\mathfrak{p})$

Example:

- $K = \mathbb{Q},\ \mathcal{O}_K = \mathbb{Z},\ \mathfrak{p} = (17) \Rightarrow$ residue field $\mathcal{O}_K \,/\, \mathfrak{p} = \mathbb{Z}\,/(17) = \mathbb{F}_{17}$
- $K = \mathbb{Q}(i),\ \mathcal{O}_K = \mathbb{Z}[i],\ \mathfrak{p} = (2+i),\ \mathcal{O}_K \,/\, \mathfrak{p} = \mathbb{F}_5$ (representatives 0,1,i+1,2,2+i)
  If $\mathfrak{p} = (3)$, $\mathcal{O}_K \,/\, \mathfrak{p} = \mathbb{F}_9(=$ "$\mathbb{F}_3[i]$)" (see picture)

- $K = \mathbb{Q}(\sqrt{d}) \quad d \equiv 2, 3 \bmod 4$ (for simplicity) $\quad \mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$
  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 some root of $X^2 - d$ over $\mathbb{F}_p$
  $$\Rightarrow \quad \mathcal{O}_K \,/\, \mathfrak{p} = \begin{cases} \mathbb{F}_p & \text{if } d \text{ is a squre mod } p \\ \mathbb{F}_{p^2} & \text{otherwise} \end{cases}$$

Notation: If $0 \neq \mathfrak{a} \trianglelefteq \mathcal{O}_K$, we say
$$x \equiv y \mod \mathfrak{a} \tag{1.2}$$
(e.g. $3 \equiv i \mod (2+i)$ in the first example)

Theorem 1.20 (Chinese Remainder Theorem)
K number field, $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ distinct primes. Then
$$\mathcal{O}_K \,/\, \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k} \to \mathcal{O}_K \,/\, \mathfrak{p}_1^{n_1} \times \cdots \times \mathcal{O}_K \,/\, \mathfrak{p}_k^{n_k} \tag{1.3}$$
$$x \mod \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k} \mapsto (x \mod \mathfrak{p}_1^{n_1}, \ldots, x \mod \mathfrak{p}_k^{n_k}) \tag{1.4}$$
is a ring isomorphism

Proof
Define $\psi : \mathcal{O}_K \to \mathcal{O}_K \,/\, \mathfrak{p}_1^{n_1} \times \cdots \times \mathcal{O}_K \,/\, \mathfrak{p}_k^{n_k}$ by $\psi(x) = (x \mod \mathfrak{p}_1^{n_1}, \ldots, x \mod \mathfrak{p}_k^{n_k})$
Then $\ker \psi = \{x \mid x \equiv 0 \mod \mathfrak{p}_i^{n_i} \ \forall i\} = \bigcup_i \mathfrak{p}_i^{n_i} = \prod_i \mathfrak{p}_i^{n_i}$ by Lemma 1.12(i)

Remains to show that ψ is surjective:
By Lemma 1.12(ii),

$$\begin{aligned} &\mathfrak{p}_j^{n_j} + \textstyle\prod_{i\neq j} \mathfrak{p}_i^{n_i} = \mathcal{O}_K \\ \Rightarrow\ &\exists \alpha \in \mathfrak{p}_j^{n_j},\ \beta \in \textstyle\prod_{i\neq j} \mathfrak{p}_i^{n_i} \text{ s.t. } \alpha+\beta = 1 \\ \Rightarrow\ &\begin{cases} \beta \equiv 0 \mod \mathfrak{p}_i^{n_i}\ \forall i \neq j \\ \beta \equiv 1 \mod \mathfrak{p}_j^{n_j} \end{cases} \end{aligned}$$

Thus $(0,\dots,0,1,0,\dots,0) \in \operatorname{Im}\psi\ \forall j$ (1 at j-th place) $\Rightarrow$ ψ surjective $\square$

Remark: Chinese Remainder Theorem implies that we can solve any system of congrueces

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

(This is called the Weak Approximation Theorem)

Lemma 1.21
$\mathfrak{p} \trianglelefteq \mathcal{O}_K$ prime ideal

(i) $|\,\mathcal{O}_K \,/\, \mathfrak{p}^n\,| = N(\mathfrak{p})^n$ (think as "$|\,\mathbb{F}_\mathfrak{p}\,|$")
(ii) $\mathfrak{p}^n \,/\, \mathfrak{p}^{n+1} \cong \mathcal{O}_K \,/\, \mathfrak{p}$ as an $\mathcal{O}_K$-module (as an abelian group)

Proof
(ii)⇒(i): $|\,\mathcal{O}_K \,/\, \mathfrak{p}^n\,| = |\,\mathcal{O}_K \,/\, \mathfrak{p}\,|\,|\,\mathfrak{p} \,/\, \mathfrak{p}^2\,| \cdots |\,\mathfrak{p}^{n-1} \,/\, \mathfrak{p}^n\,| = N(\mathfrak{p})^n$

(ii): By unique factorisation $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$, so take $\pi \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$ (i.e. $\mathfrak{p}^n \,|\, (\pi)$, $\mathfrak{p}^{n+1} \nmid (\pi)$)
Let $\phi : \mathcal{O}_K \to \mathfrak{p}^n \,/\, \mathfrak{p}^{n+1}$ by $\phi(x) = \pi x \mod \mathfrak{p}^{n+1}$

$$\ker\phi = \{x \mid \pi x \in \mathfrak{p}^{n+1}\} = \{x \mid \mathfrak{p}^{n+1} \,|\, (\pi)(x)\} = \{x \mid \mathfrak{p} \,|\, (x)\} = \mathfrak{p} \tag{1.5}$$
$$\operatorname{Im}\phi = \mathfrak{p}^n \,/\, \mathfrak{p}^{n+1} \tag{1.6}$$
$$\text{since } (\pi) + \mathfrak{p}^{n+1} = \mathfrak{p}^n \text{ by Lemma (1.12)(ii)} \tag{1.7}$$

By First Isomorphism Theorem, $\mathcal{O}_K \,/\, \mathfrak{p} \xrightarrow{\sim} \mathfrak{p}^n \,/\, \mathfrak{p}^{n+1}$ $\square$

Corollary 1.22
$N(\mathfrak{a}\,\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$

Proof
Follows from Theorem 1.20 and Lemma 1.21 $\square$

Corollary 1.23
$\mathfrak{a} \ni N(\mathfrak{a})$ (True for prime ideals, as char $\mathcal{O}_K \,/\, \mathfrak{p} \equiv 0 \mod \mathfrak{p}$, so $|\,\mathcal{O}_K \,/\, \mathfrak{p}\,| \in \mathfrak{p}$, and use multiplicativity)

(In fact, this is obvious anyway as $N(\mathfrak{a})$ must be zero in any abelian group of order $N(\mathfrak{a})$. In particular, in $\mathcal{O}_K \,/\, \mathfrak{a}$; i.e. $\mathfrak{a} \ni N(\mathfrak{a})$)

1.6 Extending the Number Field

Example: $\mathbb{Q}(i)/\,\mathbb{Q}$ Take primes in $\mathbb{Q}$ and factorise in $\mathbb{Q}(i)$

$$2\,\mathbb{Z}[i] = \quad (2) \quad = (1+i)^2 \qquad \leftarrow 2 \text{ ramifies} \tag{1.8}$$
$$3\,\mathbb{Z}[i] = \quad (3) \quad \text{is prime} \qquad \leftarrow 3 \text{ inert} \tag{1.9}$$
$$5\,\mathbb{Z}[i] = \quad (5) \quad = (2+i)(2-i) \qquad \leftarrow 5 \text{ splits} \tag{1.10}$$

Note that $\mathfrak{p} \ni N(\mathfrak{p})$ and hence some prime number p, so $p|(p)$. Thus factorising $2, 3, 5, 7, \ldots$ yields all the primes of $\mathbb{Q}(i)$

Definition 1.24
Let L/K be an extension of number fields, and $\mathfrak{a} \trianglelefteq \mathcal{O}_K$ ideal.
Then conorm of $\mathfrak{a}$ is the ideal $\mathfrak{a}\,\mathcal{O}_L$ of $\mathcal{O}_L$ the ideal generated by the elements of $\mathfrak{a}$ in $\mathcal{O}_L$
Equivalently, if $\mathfrak{a} = (\alpha_1, \ldots, \alpha_n)$ as an $\mathcal{O}_K$-ideal, then $\mathfrak{a}\,\mathcal{O}_L = (\alpha_1, \ldots, \alpha_n)$ as an $\mathcal{O}_L$-ideal

Note:

$$(\mathfrak{a}\,\mathcal{O}_L)(\mathfrak{b}\,\mathcal{O}_L) = (\mathfrak{a}\,\mathfrak{b})\,\mathcal{O}_L$$
$$\mathfrak{a}\,\mathcal{O}_M = (\mathfrak{a}\,\mathcal{O}_L)\,\mathcal{O}_M \text{ when } K \subseteq L \subseteq M$$

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

Proposition 1.25
L/K extension of number fields, $\mathfrak{a} \subseteq \mathcal{O}_K$ a non-zero ideal. Then

$$N(\mathfrak{a}\,\mathcal{O}_L) = N(\mathfrak{a})^{[L:K]} \tag{1.11}$$

Proof
If $\mathfrak{a} = (\alpha)$ is principal, then (by Lemma 1.16)

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

so all ok. In general, $\mathfrak{a}^k = (\alpha)$ for some k, (since Cl_K is finite)
Hence $N(\mathfrak{a}\,\mathcal{O}_L)^k = N(\mathfrak{a})^{k[L:K]}$, and so $N(\mathfrak{a}\,\mathcal{O}_L) = N(\mathfrak{a})^{[L:K]}$ $\square$

Definition 1.26
A prime $\mathfrak{q}$ of L lies above a prime $\mathfrak{p}$ of K if $\mathfrak{q} \,|\, \mathfrak{p}\,\mathcal{O}_L$
(Equivalently, if $\mathfrak{p}\,\mathcal{O}_L = \mathfrak{q} \times$ "other stuff"
Equivalently, if $\mathfrak{q} \supseteq \mathfrak{p}$)

Lemma 1.27
L/K number fields. Every prime of L lies above a unique prime of K: $\mathfrak{q}$ lies above $\mathfrak{q} \cap \mathcal{O}_K$

Proof
$\mathfrak{q} \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$, and it is non-zero as, for example, it contains $N(\mathfrak{q})$ (Corollary 1.23).
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 $\mathfrak{q} \supseteq \mathfrak{p} + \mathfrak{p}' = \mathcal{O}_K \ni \{1\}$ $\quad \#$ $\square$

Lemma 1.28
Suppose $\mathfrak{q} \trianglelefteq \mathcal{O}_K$ lies above $\mathfrak{p} \trianglelefteq \mathcal{O}_K$
Then $\mathcal{O}_L\,/\,\mathfrak{q}$ is a field extension of $\mathcal{O}_K\,/\,\mathfrak{p}$

Proof
Define

$$\phi : \mathcal{O}_K / \mathfrak{p} \;\to\; \mathcal{O}_L / \mathfrak{q} \tag{1.12}$$
$$x \mod \mathfrak{p} \;\mapsto\; x \mod \mathfrak{q} \tag{1.13}$$

This is well-defined as $\mathfrak{q} \supseteq \mathfrak{p}$
This is ring homomorphism (and $1 \mapsto 1$), so has no kernel as $\mathcal{O}_K / \mathfrak{p}$ is a field, i.e. an embedding $\mathcal{O}_K / \mathfrak{p} \hookrightarrow \mathcal{O}_L / \mathfrak{q}$ $\square$

Note (to the proof): The "reduction mod $\mathfrak{q}$" map in $\mathcal{O}_L$ extends the "reduction mod $\mathfrak{p}$" map in $\mathcal{O}_K$

Example: $\mathbb{Q}(i)/\mathbb{Q}$
$p = 3$ $\quad \mathfrak{p} = (3)$
Note that $n\,\mathbb{Z}[i] = (n)\,\mathcal{O}_L$ has norm $n^2 = n^{[\mathbb{Q}(i):\mathbb{Q}]}$ (c.f. Proposition 1.25)

Definition 1.29
If $\mathfrak{q}$ lies above $\mathfrak{p}$, then its residue degree is $f_{\mathfrak{q}/\mathfrak{p}} = [\mathcal{O}_L / \mathfrak{q} : \mathcal{O}_K / \mathfrak{p}]$
Its ramification degree is the exponent $e_{\mathfrak{q}/\mathfrak{p}}$ in the prime factorisation $\mathfrak{p}\,\mathcal{O}_L = \mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}} \prod(\text{other primes})$

Theorem 1.30
L/K an extension of number fields, $\mathfrak{p}$ a prime of K

(i) If $\mathfrak{p}\,\mathcal{O}_L$ decomposes as $\mathfrak{p}\,\mathcal{O}_L = \prod_{i=1}^m \mathfrak{q}_i^{e_i}$ ($\mathfrak{q}_i$ distinct, $e_i = e_{\mathfrak{q}_i/\mathfrak{p}}, f_i = f_{\mathfrak{q}_i/\mathfrak{p}}$). Then

$$\sum_{i=1}^m e_i f_i = [L : K] \tag{1.14}$$

(ii) If M/L a further field extension, $\mathfrak{r}$ lies above $\mathfrak{q}$ lies above $\mathfrak{p}$ (in M, L, K respectively) Then

$$e_{\mathfrak{r}/\mathfrak{q}} e_{\mathfrak{q}/\mathfrak{p}} = e_{\mathfrak{r}/\mathfrak{p}} \tag{1.15}$$
$$\text{and} \quad f_{\mathfrak{r}/\mathfrak{q}} f_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{r}/\mathfrak{p}} \tag{1.16}$$

Proof

(i) $N(\mathfrak{p})^{[L:K]} =$ (Prop1.25) $N(\mathfrak{p}\,\mathcal{O}_L) = N(\prod \mathfrak{q}_i^{e_i}) =$ (Cor1.22) $\prod N(\mathfrak{q}_i)^{e_i} = \prod N(\mathfrak{q})^{f_i e_i} = N(\mathfrak{q})^{\sum e_i f_i}$

(ii) Multiplicativity of e follows by writing out the prime decomposition of $\mathfrak{p}\,\mathcal{O}_M$. That of f is the Tower Law: $[\mathcal{O}_M / \mathfrak{r} : \mathcal{O}_L / \mathfrak{q}][\mathcal{O}_L / \mathfrak{q} : \mathcal{O}_K / \mathfrak{p}] = [\mathcal{O}_M / \mathfrak{r} : \mathcal{O}_K / \mathfrak{p}]$

$\square$

Definition 1.31
L/K extension of number fields, $\mathfrak{p}$ a prime of K with $\mathfrak{p}\,\mathcal{O}_L = \prod_{i=1}^m \mathfrak{q}_i^{e_i}$
Then $\mathfrak{p}$ splits completely in L if $m = [L : K]$, $m > 1$ ($\Rightarrow e_i = f_i = 1$)
and $\mathfrak{p}$ is totally ramified in L if $m = f_1 = 1, e_1 = [L : K]$
We will see that when L/K is Galois then $e_i = e_j, f_i = f_j \; \forall i, j$. Then, say $\mathfrak{p}$ is ramified at $e_1 > 1$ (being unambiguous) or is unramified if $e_1 = 1$

Example:
5 splits (completely) in $\mathbb{Q}(i)/\mathbb{Q}$ ($5 = (2+i)(2-i)$)
2 is (totally) ramified in $\mathbb{Q}(i)/\mathbb{Q}$ ($2 = (1+i)^2$)
p is totally ramified in $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$, ζ_{p^n}=prime p^n-th root of unity

Theorem 1.32 (Kummer-Dedekind)
L/K an extension of number fields.
Suppose $[\mathcal{O}_L : \mathcal{O}_K[\alpha]] = N < \infty$ for some algebraic integer $\alpha \in \mathcal{O}_L$ with minimal polynomials $f(X) \in \mathcal{O}_K[X]$
Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal s.t. $\mathfrak{p} \nmid N$ ($\Rightarrow \operatorname{char} \mathcal{O}_K / \mathfrak{p} \nmid N$)

If $\quad f(X) \mod \mathfrak{p} = \prod_{i=1}^{m} \bar{g}_i(X)^{e_i} \quad$ ($\bar{g}_i$ distinct irreducible)

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

where $\quad g_i(X) \in \mathcal{O}_K[X]$ s.t. $\bar{g}_i(X) = g_i(X) \mod \mathfrak{p}$
and $\mathfrak{q}_i$ are distinct primes of L with $e_{\mathfrak{q}_i/\mathfrak{p}} = e_i$ and $f_{\mathfrak{q}_i/\mathfrak{p}} = \deg \bar{g}_i$

Example:
$K = \mathbb{Q} \quad L = \mathbb{Q}(\zeta_5) \quad \zeta = \zeta_5$ =primitive 5-th root of unity $\quad \mathcal{O}_L = \mathbb{Z}[\zeta]$
Take $\alpha = \zeta$, so $N = 1$, $f(X) = X^4 + X^3 + X^2 + X + 1$
$f(X) \mod 2$ is irreducible $\Rightarrow$ (2) is prime in $\mathcal{O}_L$, residue field is $\mathbb{F}_{16}$
$f(X) \mod 3$ is irreducible $\Rightarrow$ (3) is prime in $\mathcal{O}_L$, residue field is $\mathbb{F}_{81}$
$f(X) \mod 5 = (X-1)^4 \quad \Rightarrow \quad (5) = (5, \zeta - 1)^4$
$f(X) \mod 7$ is irreducible
$f(X) \mod 11 = (X-4)(X-9)(X-5)(X-3) \quad \Rightarrow \quad (11) = (11, \zeta-4)(11, \zeta-9)(11, \zeta-5)(11, \zeta-3)$
$f(X) \mod 19 = (X^2+5X+1)(X^2-4X+1) \quad \Rightarrow \quad (19) = (19, \zeta^2+5\zeta+1)(19, \zeta^2-4\zeta+1)$

Example:
$K = \mathbb{Q} \quad L = \mathbb{Q}(\zeta_{p^n}) \quad \zeta = \zeta_{p^n}$ =primitive p^nth root of unity and p prime
minimal polynomial $f(X) = \frac{X^{p^n}-1}{X^{p^{n-1}}-1} \equiv (X-1)^{p^n - p^{n-1}} \mod p \quad \Rightarrow \quad p$ is totally ramified in $\mathbb{Q}(\zeta)/\mathbb{Q}$
If $q \neq p$ is also prime, $\quad \gcd(X^{p^n} - 1 \mod q, \frac{d}{dx}(X^{p^n} - 1) \mod q) = 1$
$\Rightarrow \quad X^{p^n} - 1 \mod q$ has no repeated roots (in $\overline{\mathbb{F}_q}$)
$\Rightarrow \quad f(X) \mod q$ has no repeated roots
$\Rightarrow \quad$ all $e_i = 1$, $\quad$ i.e. q is unramified in $\mathbb{Q}(\zeta)$

Remark:
Cannot always find α s.t. $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ (i.e. $N = 1$)
However, by the Primitive Element Theorem, can find α s.t. $L = K(\alpha)$. Scalar α (by an integer) can ensure that $\alpha \in \mathcal{O}_L$. Then $\mathcal{O}_L[\alpha]$ has finite index in $\mathcal{O}_L$
Therefore, the theorem allows us to decompose all except possibly a finite number of primes.

Proof of Kummer-Dedekind Theorem
Write $A = \mathcal{O}_K[\alpha]$, $\mathbb{F} = \mathcal{O}_K \,/\, \mathfrak{p}$, $p = \operatorname{char} \mathbb{F}$

- $$\begin{aligned} \alpha \quad &\leftarrow\!\shortmid \quad x && (1.17)\\ A/(\mathfrak{p}\, A + g_i(\alpha)A) \quad &\overset{\sim}{\longleftarrow} \quad \mathcal{O}_K[X]/(f(X), \mathfrak{p}, g_i(X)) \\ &\cong \mathbb{F}[X]/(\bar{f}(X), \bar{g}_i(X)) \\ &= \mathbb{F}[X]/(\bar{g}_i(X)) && (1.18)\end{aligned}$$
  a field af degree $f_i = \deg \bar{g}_i$ over $\mathbb{F}$ $\quad$ ($\bar{g}_i$ is irreducible)

- Pick $M \in \mathbb{Z}$ s.t. $NM \equiv 1 \mod p$, and consider
$$\phi : A/\,\mathfrak{p}\, A + g_i(\alpha)A \quad \rightarrow \quad \mathcal{O}_L \,/\, \mathfrak{q}_i \tag{1.19}$$
$$\phi(x \mod \mathfrak{p}\, A + g_i(\alpha)A) \quad = \quad x \mod \mathfrak{q}_i \tag{1.20}$$

<u>ϕ well-defined:</u> Since $\mathfrak{q}_i \supseteq \mathfrak{p}\, A + g_i(\alpha)A$
<u>ϕ is surjective:</u> If $x \in \mathcal{O}_L$, then $Nx \in A$ and
$$\phi(MNx) \quad = \quad MNx \mod \mathfrak{q}_i \tag{1.21}$$
$$= \quad x \mod \mathfrak{q}_i \tag{1.22}$$

as $MN \equiv 1 \mod \mathfrak{q}_i \ni p$
$\mathcal{O}_L \,/\, \mathfrak{q}_i$ is non-zero, otherwise $1 \in \mathfrak{p}\, \mathcal{O}_L + g_i(\alpha)\, \mathcal{O}_L$
$\Rightarrow$ both p and $MN \in \mathfrak{p}\, A + g_i(\alpha)A$
$\Rightarrow$ $1 \in \mathfrak{p}\, A + g_i(\alpha)A$ $\quad$ # to step 1
$\Rightarrow$ ϕ is an isomorphism
$\Rightarrow$ $\mathcal{O}_L \,/\, \mathfrak{q}_i$ is a field extension of $\mathbb{F}$ of degree $f_i = \deg \bar{g}_i$ and $\mathfrak{q}_i$ is prime

- For $i \neq j$, as $\gcd(\bar{g}_i(X), \bar{g}_j(X)) = 1$, $\quad \exists \lambda(X), \mu(X) \in \mathcal{O}_K[X]$ s.t.
$$\lambda(X)g_i(X) + \mu(X)g_j(X) \equiv 1 \mod \mathfrak{p} \tag{1.23}$$
Then $\mathfrak{q}_i + \mathfrak{q}_j$ contains both $\mathfrak{p}$ and $\lambda(\alpha)g_i(\alpha) + \mu(\alpha)g_j(\alpha) \equiv 1 \mod \mathfrak{p}$
$\Rightarrow$ $\mathfrak{q}_i + \mathfrak{q}_j = \mathcal{O}_L$ $\quad \Rightarrow$ $\mathfrak{q}_i \neq \mathfrak{q}_j$ for $i \neq j$

- $$\begin{aligned} \prod_i \mathfrak{q}_i^{e_i} \quad &= \quad \prod_i \left(\mathfrak{p}\, \mathcal{O}_L + g_i(\alpha)\, \mathcal{O}_L\right)^{e_i} && (1.24)\\ &\subseteq \quad \mathfrak{p}\, \mathcal{O}_L + \left(\prod_i g_i(\alpha)^{e_i}\right) \mathcal{O}_L && (1.25)\\ &= \quad \mathfrak{p}\, \mathcal{O}_L \quad \text{since} \quad \prod g_i(\alpha)^{e_i} \equiv f(\alpha) = 0 \mod \mathfrak{p} && (1.26)\end{aligned}$$

But
$$\begin{aligned} N(\prod_i \mathfrak{q}_i^{e_i}) \quad &= \quad \prod_i \left(|\,\mathbb{F}\,|^{f_i}\right)^{e_i} \quad \text{(by Step 2)} \\ &= \quad |\,\mathbb{F}\,|^{\sum e_i f_i} \; = \; |\,\mathbb{F}\,|^{\deg f} \; = \; |\,\mathbb{F}\,|^{[L:K]} \\ &= \quad N(\mathfrak{p}\, \mathcal{O}_L) \quad \text{by Proposition 1.25} && (1.27)\\ \Rightarrow \quad \prod_{i=1}^{m} \mathfrak{q}_i^{e_i} \quad &= \quad \mathfrak{p}\, \mathcal{O}_L && (1.28)\end{aligned}$$

$\square$

Proposition 1.33
$L/\mathbb{Q}$ finite extension, $\alpha \in \mathcal{O}_L$ with $L = \mathbb{Q}(\alpha)$ minimal polynomial $f(X) \in \mathbb{Z}[X]$. If $f(X) \mod p$ has distinct roots (in $\overline{\mathbb{F}}_p$) then $[\mathcal{O}_L : \mathbb{Z}[\alpha]]$ is coprime to p (so Kummer-Dedekind Theorem applies)

Proof
Let F=splitting field of f, $f(X) = \prod_i (X - \alpha_i) \quad \alpha_i \in F$
Fix $\mathfrak{p}$ a prime in F above (p).
As $f(X)$ has no repeated roots in $\overline{\mathbb{F}}_p$ and $\overline{f}(X) = \prod_i (X - \overline{\alpha}_i)$ (‾ denotes reduction mod $\mathfrak{p}$)
$\Rightarrow \quad \overline{\alpha}_i$ are distinct in $\mathcal{O}_F / \mathfrak{p}$
$\Rightarrow \quad \prod_{i<j}(\alpha_i - \alpha_j) \neq 0 \mod \mathfrak{p}$
Let $\beta_1, \beta_2, \ldots, \beta_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_L$ ($n = [L : \mathbb{Q}]$)

$$\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \vdots \\ \alpha^{n-1} \end{pmatrix} = M \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} \qquad \text{for some } M \in Mat_n(\mathbb{Z}) \text{ with } \det M = [\mathcal{O}_L : \mathbb{Z}[\alpha]] \tag{1.29}$$

Writing $id = \sigma_1, \sigma_2, \ldots, \sigma_n$ for the embeddings of $L \hookrightarrow F$

$$\prod_{i>j}(\alpha_i - \alpha_j) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & & \vdots \\ \alpha_1^2 & \vdots & \cdots & \vdots \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & & \alpha_n^{n-1} \end{vmatrix} \tag{1.30}$$

$$= \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \sigma_2(\alpha_2) & & \vdots \\ \alpha_1^2 & \vdots & \cdots & \vdots \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-1} & \sigma_2(\alpha_2)^{n-1} & & \sigma_n(\alpha_n)^{n-1} \end{vmatrix} \tag{1.31}$$

$$= \det M \begin{pmatrix} \beta_1 & \sigma_2(\beta_1) & \cdots \sigma_n(\beta_1) & \\ \beta_2 & \vdots & & \vdots \\ \beta_3 & \vdots & \cdots & \vdots \\ \vdots & \vdots & & \vdots \\ \beta_n & \sigma_2(\beta_2) & & \sigma_n(\beta_n) \end{pmatrix} \tag{1.32}$$

$$= [\mathcal{O}_L : \mathbb{Z}[\alpha]]B \quad \text{for some } B \in \mathcal{O}_K \tag{1.33}$$

$$\tag{1.34}$$

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

Proposition 1.34
K number field, $\mathfrak{p}$ prime of K.
Suppose $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}_K[X]$ is Eisenstein w.r.t $\mathfrak{p}$ (i.e. $\mathfrak{p} \,|\, (a_i) \; \forall i, \quad \mathfrak{p}^2 \nmid (a_0)$)
Then $K(\alpha)/K$ has degree $n = \deg f$ and $\mathfrak{p}$ is totally ramified in $K(\alpha)$, where $f(\alpha) = 0$

Proof
see Local Fields □

2 Decomposition of Primes

2.1 Action of Galois groups

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

- F/K is normal (if $f \in K[X]$ irreducible has a root in $F \quad \Rightarrow \quad f$ splits completely in F)
- $|\,\mathrm{Gal}(F/K)| = [F : K]$
- $$\{\text{subgroup}\} \overset{\text{one-to-one}}{\longleftrightarrow} \{\text{intermediate field}\}$$

$$H \leq \mathrm{Gal}(F/K) \quad \to \quad F^H \quad (\text{fixed field of } H) \tag{2.1}$$
$$\mathrm{Gal}(F/L) \quad \leftarrow \quad K \subseteq L \subseteq F \tag{2.2}$$

Example:

Lemma 2.1
Let $g \in \mathrm{Gal}(F/K)$
$\mathfrak{q}$ prime of F above $\mathfrak{p}$, a prime of K

(i) $\alpha \in \mathcal{O}_F \quad \Rightarrow \quad g\alpha \in \mathcal{O}_F$ (so $\mathrm{Gal}(F/K)$ acts on $\mathcal{O}_F$)

(ii) $\mathfrak{a} \subseteq \mathcal{O}_F$ ideal $\quad \Rightarrow \quad g(\mathfrak{a}) \subseteq \mathcal{O}_F$ ideal

(iii) $\mathfrak{a}, \mathfrak{b}$ ideals $\quad \Rightarrow \quad g(\mathfrak{a}\,\mathfrak{b}) = g(\mathfrak{a})g(\mathfrak{b}), g(\mathfrak{a} + \mathfrak{b}) = g(\mathfrak{a}) + g(\mathfrak{b})$

(iv) $g(\mathfrak{q})$ is a prime of F above $\mathfrak{p}$ (so $\mathrm{Gal}(F/K)$ acts on the set of primes above $\mathfrak{p}$)

(v) $e_{\mathfrak{q}\,/\,\mathfrak{p}} = e_{g(\mathfrak{q})/\,\mathfrak{p}}, f_{\mathfrak{q}\,/\,\mathfrak{p}} = f_{g(\mathfrak{q})/\,\mathfrak{p}}$

Proof
Clear $\square$

Example:
$K = \mathbb{Q}$ $\quad F = \mathbb{Q}(i)$ $\quad \mathcal{O}_F = \mathbb{Z}[i]$ $\quad \mathrm{Gal}(F/K) = \{\text{id, complex conjugation}\}$

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

Proof
Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ be the primes above $\mathfrak{p}$
Require to proof: $\quad \exists g \in \mathrm{Gal}(F/K)$ s.t. $g(\mathfrak{q}_1) = \mathfrak{q}_2$
Pick $x \in \mathcal{O}_F$ s.t. $\begin{array}{lcl} x & \equiv & 0 \mod \mathfrak{q}_1 \\ x & \not\equiv & 0 \mod \mathfrak{q}_i \,\forall i \neq 1 \end{array}$
(this is possible by Chinese Remainder Theorem)
Then

$$\prod_{h \in \mathrm{Gal}(F/K)} h(x) \in K \cap \mathcal{O}_F \cap \mathfrak{q}_1 = \mathcal{O}_K \cap \mathfrak{q}_1 = \mathfrak{p} \subseteq \mathfrak{q}_2 \tag{2.3}$$

$$\begin{array}{lrl} \Rightarrow & g(x) \equiv 0 \mod \mathfrak{q}_2 & \text{for some } g \\ \Rightarrow & x \equiv 0 \mod g^{-1}(\mathfrak{q}_2) & \\ \Rightarrow & g^{-1}(\mathfrak{q}_2) = \mathfrak{q}_1 & \text{by choice of } x \\ \Rightarrow & \mathfrak{q}_2 = g(\mathfrak{q}_1) & \end{array}$$

□

Corollary 2.3
F/K Galois.
If $\mathfrak{q}_1, \mathfrak{q}_2$ lie above $\mathfrak{p}$, then $\begin{cases} e_{\mathfrak{q}_1/\mathfrak{p}} = e_{\mathfrak{q}_2/\mathfrak{p}} \\ f_{\mathfrak{q}_1/\mathfrak{p}} = f_{\mathfrak{q}_2/\mathfrak{p}} \end{cases}$ (So can write $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$ without ambiguity)

2.2 Decomposition Groups

Definition 2.4
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 $D_{\mathfrak{q}} (= D_{\mathfrak{q}\,/\,\mathfrak{p}})$ of $\mathfrak{q}$ (over $\mathfrak{p}$) i.e.

$$D_{\mathfrak{q}\,/\,\mathfrak{p}} = \mathrm{Stab}_{\mathrm{Gal}(F/K)}(\mathfrak{q}) \tag{2.4}$$

Remark. The decomposition group determines how $\mathfrak{p}$ decomposes in all intermediate extensions.

Example 2.5
$\mathrm{Gal}(F/K) = S_4 \qquad D_{\mathfrak{q}\,/\,\mathfrak{p}} = S_3 < S_4$
$\Rightarrow \exists 4$ primes above $\mathfrak{p}$ (by Orb-Stab Theorem)
and action of S_4 on these is the usual action on 4 points

Consider $H = \{\mathrm{id}, (12)(34)\} \leq S_4$ and $L = F^H$
$\mathrm{Gal}(F/L)$ acts transitively on the primes of F above every prime of L
$\Rightarrow$ number of primes in L above $\mathfrak{p}$ = number of H-orbits on $\{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_4\} = 2$

Remark. If G is a finite group

$$\{\text{transitive } G\text{-sets}\}/\cong \quad \longleftrightarrow \quad \{\text{subgroup of } G\}/\text{conjugacy} \tag{2.5}$$
$$X \quad \longmapsto \quad \mathrm{Stab}(x) \tag{2.6}$$
$$G/H \quad \longleftarrow\!\shortmid \quad H \tag{2.7}$$

Number of primes in F^H above $\mathfrak{p}$ = number of H-orbits on $\{\text{primes above } \mathfrak{p}\}$ = number of H-orbits on $G/D_{\mathfrak{q}\,/\,\mathfrak{p}}$ = number of double cosets HxD

Note:
Double coset HxD for $x \in G$ is the set $\{hxd | h \in H, d \in D\}$
$G = \bigsqcup$ double cosets
If $y \in HxD \quad \Rightarrow \quad HyD = HxD$
Warning: double cosets can have different sizes, unlike coset

$g \in D_{\mathfrak{q}}$ fixes $\mathfrak{q} \quad \Rightarrow \quad$ it acts on $\mathcal{O}_F\,/\,\mathfrak{q}$ by

$$x \mod \mathfrak{q} \mapsto g(x) \mod \mathfrak{q} \tag{2.8}$$

This gives a natural map

$$D_{\mathfrak{q}} \longrightarrow \mathrm{Gal}((\mathcal{O}_F\,/\,\mathfrak{q})/(\mathcal{O}_K\,/\,\mathfrak{p})) \tag{2.9}$$

(think it as $\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}\,/\,\mathbb{F}_{\mathfrak{p}})$)

Example:
$F = \mathbb{Q}(i) \qquad K = \mathbb{Q} \qquad p = 3$

$\mathrm{Gal}(F/\,\mathbb{Q}) = \{\mathrm{id}, c\}$ where c =complex conjugate$\in D_{(3)}$
Complex conjugation acts as $(a + bi \mod 3) \mapsto (a - bi \mod 3) = ((a + bi)^3 \mod 3)$
which is the Frobenius automorphism $x \mapsto x^3$ on $\mathbb{F}_9$

Theorem 2.6
F/K Galois, $\mathfrak{q}$ prime of F above $\mathfrak{p}$ prime of K
Then the natural map

$$D_{\mathfrak{q}} \longrightarrow \mathrm{Gal}((\mathcal{O}_F \,/\, \mathfrak{q})/(\mathcal{O}_K \,/\, \mathfrak{p})) \tag{2.10}$$

is surjective

Proof
$\beta \in \mathcal{O}_F \,/\, \mathfrak{q}$ with $\mathcal{O}_F \,/\, \mathfrak{q} = \mathcal{O}_K \,/\, \mathfrak{p}[\beta]$ (e.g. a generator for $(\mathcal{O}_F \,/\, \mathfrak{q})^\times$)
Let $f(x) \in \mathcal{O}_K \,/\, \mathfrak{p}[X]$ be its minimal polynomial and $\beta = \beta_1, \beta_2, \ldots, \beta_n \in \mathcal{O}_F \,/\, \mathfrak{q}$ its roots
Sufficient to proof: $\exists g \in \mathrm{Gal}(F/K)$ with $g(\mathfrak{q}) = \mathfrak{q}$ and $g(\beta) = \beta_2$

Pick $\alpha \in \mathcal{O}_F$ with $\alpha \mod \mathfrak{q} = \beta, \alpha \mod \mathfrak{q}' = 0$ for all other prime $\mathfrak{q}'$ above $\mathfrak{p}$ (this is okay by CRT)
Let $\mathcal{F}(X) \in \mathcal{O}_K[X]$ be its minimal polynomial over K
and $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r \in \mathcal{O}_K$ be its roots (note F/K normal $\Rightarrow$ all roots are in F)

$\mathcal{F}(X) \mod \mathfrak{p}$ has β as a root
$\Rightarrow \mathcal{F}(X) \mod \mathfrak{p}$ is divisible by $f(X)$
$\Rightarrow \mathcal{F}(X) \mod \mathfrak{p}$ has β_2 as a root

WLOG $\alpha_2 \mod \mathfrak{q} = \beta_2$
Now take $g \in \mathrm{Gal}(F/K)$ s.t. $g(\alpha) = \alpha_2$
Then $g(\alpha) \neq 0 \mod \mathfrak{q} \quad \Rightarrow \quad g(\mathfrak{q}) = \mathfrak{q}$ and $g(\beta) = \beta_2$ $\square$

Corollary 2.7
K number fields, F/K splitting field of monic irreducible $f(X) \in \mathcal{O}_K[X]$
Let $\mathfrak{p}$ be a prime of K and assume

$$f(X) \mod \mathfrak{p} = g_1(X) g_2(X) \cdots g_k(X) \tag{2.11}$$

with $g_i(X) \in \mathcal{O}_K \,/\, \mathfrak{p}[X]$ distinct irreducible, with degree $\deg g_i = d_i$
Then $\quad \mathrm{Gal}(F/K) \leq S_n \quad (n = \deg f)$ has an element of cycle type $(d_1, d_2, \ldots, d_k)$

Proof
Let $\mathfrak{q}$ be a prime above $\mathfrak{p}$ and let $\alpha_1, \ldots, \alpha_n \in F$ be the roots of f.
$f(\alpha_i \mod \mathfrak{q}) \mod \mathfrak{p} = 0 \ \forall i \qquad$ and $\qquad \alpha_i \mod \mathfrak{p}$ distinct (since g_i distinct)
$\Rightarrow \quad$ action of $D_{\mathfrak{q}\,/\,\mathfrak{p}}$ on $\alpha_1, \ldots, \alpha_n =$ action on the roots of $f \mod \mathfrak{p}$
Now take g which maps to the generator $\mathrm{Gal}((\mathcal{O}_F \,/\, \mathfrak{q})/(\mathcal{O}_K \,/\, \mathfrak{p}))$
$\Rightarrow \quad g$ has the correct cycle type on the α_i $\square$

Definition 2.8
F/K Galois, $\mathfrak{q}$ a prime above $\mathfrak{p}$
The inertia subgroup (at $\mathfrak{q}$), denote $I_{\mathfrak{q}} = I_{\mathfrak{q}\,/\,\mathfrak{p}}$ is the (normal) subgroup of $D_{\mathfrak{q}}$ that acts trivially on $\mathcal{O}_F \,/\, \mathfrak{q}$, i.e.

$$I_{\mathfrak{q}} = \ker\left(D_{\mathfrak{q}} \twoheadrightarrow \mathrm{Gal}((\mathcal{O}_F \,/\, \mathfrak{q})/(\mathcal{O}_K \,/\, \mathfrak{p}))\right) \tag{2.12}$$

$D_{\mathfrak{q}} \twoheadrightarrow \mathrm{Gal}((\mathcal{O}_F \,/\, \mathfrak{q})/(\mathcal{O}_K \,/\, \mathfrak{p}))$ surjective $\Rightarrow D_{\mathfrak{q}}/I_{\mathfrak{q}} \cong \mathrm{Gal}((\mathcal{O}_F \,/\, \mathfrak{q})/(\mathcal{O}_K \,/\, \mathfrak{p}))$

We also have

$$\mathrm{Gal}((\mathcal{O}_F \,/\, \mathfrak{q})/(\mathcal{O}_K \,/\, \mathfrak{p})) \cong \mathbb{Z} \,/ m\, \mathbb{Z} \cong \langle \phi \rangle \tag{2.13}$$

where ϕ is the Frobenius map $\phi(x) = x^{N(\mathfrak{p})}$ and $m =$order of $N(\mathfrak{p})$ in $\mathcal{O}_K \,/\, \mathfrak{p}$
The (arithmetic) Frobenius element is $\mathrm{Frob}_{\mathfrak{q}\,/\,\mathfrak{p}} \in D_{\mathfrak{q}}/I_{\mathfrak{q}}$ s.t. $\mathrm{Frob}_{\mathfrak{q}\,/\,\mathfrak{p}} \mapsto \phi$ under the induced map

Note: In Corollary 2.7, $I_{\mathfrak{q}\,/\,\mathfrak{p}}$ is trivial and $\mathrm{Frob}_{\mathfrak{q}\,/\,\mathfrak{p}}$ acts as the element of S_n of cycle type $(d_1, \ldots, d_n)$

Theorem 2.9
F/K Galois extension of number field, $\mathfrak{q}$ a prime of F above $\mathfrak{p}$ a prime of K. Then

(i) $\left|D_{\mathfrak{q}\,/\,\mathfrak{p}}\right| = e_{\mathfrak{q}\,/\,\mathfrak{p}} f_{\mathfrak{q}\,/\,\mathfrak{p}}$

(ii) The order of $\mathrm{Frob}_{\mathfrak{q}\,/\,\mathfrak{p}} = f_{\mathfrak{q}\,/\,\mathfrak{p}}$

(iii) $\left|I_{\mathfrak{q}\,/\,\mathfrak{p}}\right| = e_{\mathfrak{q}\,/\,\mathfrak{p}}$

If L an intermediate field, $\mathfrak{s}$ a prime of L below $\mathfrak{q}$, then

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

(ii) $I_{\mathfrak{q}\,/\mathfrak{s}} \;=\; I_{\mathfrak{q}\,/\,\mathfrak{p}} \cap \mathrm{Gal}(F/L)$

Proof

(i) If n =number of primes above $\mathfrak{p}$, then

$$\begin{aligned} n\left|D_{\mathfrak{q}\,/\,\mathfrak{p}}\right| &= \left|\,\mathrm{Gal}(F/K)\right| && \text{(by Orb-Stab and transitivity)} && (2.14)\\ &= [F:K] \;=\; n e_{\mathfrak{q}\,/\,\mathfrak{p}} f_{\mathfrak{q}\,/\,\mathfrak{p}} && \text{(by Theorem1.30 and Corollary 2.3)} && (2.15) \end{aligned}$$

(ii) $f_{\mathfrak{q}\,/\,\mathfrak{p}} = [\mathcal{O}_F\,/\,\mathfrak{q} : \mathcal{O}_K\,/\,\mathfrak{p}] = \left|\,\mathrm{Gal}((\mathcal{O}_F\,/\,\mathfrak{q})/(\mathcal{O}_L\,/\,\mathfrak{p}))\right| = \text{order of } \mathrm{Frob}_{\mathfrak{q}\,/\,\mathfrak{p}}$

(iii) $\left|D_{\mathfrak{q}\,/\,\mathfrak{p}}\right| = \left|I_{\mathfrak{q}\,/\,\mathfrak{p}}\right| \cdot \text{order of } \mathrm{Frob}_{\mathfrak{q}\,/\,\mathfrak{p}} \quad \Rightarrow \quad \left|I_{\mathfrak{q}\,/\,\mathfrak{p}}\right| = \frac{e_{\mathfrak{q}\,/\,\mathfrak{p}} f_{\mathfrak{q}\,/\,\mathfrak{p}}}{f_{\mathfrak{q}\,/\,\mathfrak{p}}}$

The rests are straight forward from definition $\square$

Example:
$K = \mathbb{Q} \qquad F = \mathbb{Q}(\zeta_n) \qquad \zeta_n$ =primitive n-th root of unity
Let $p \nmid n$ be a prime number, $\mathfrak{q}$ a prime of F above p
p is unramified $\quad\Rightarrow\quad I_{\mathfrak{q}\,/\,\mathfrak{p}} = \{\mathrm{id}\}$ and $D_{\mathfrak{q}\,/\,\mathfrak{p}} = \langle \mathrm{Frob}_{\mathfrak{q}\,/\,\mathfrak{p}} \rangle$
$\mathrm{Frob}_{\mathfrak{q}\,/\,\mathfrak{p}}$ acts $x \mapsto x^p$ on $\mathcal{O}_F\,/\,\mathfrak{q}$
$\Rightarrow \quad \mathrm{Frob}_{\mathfrak{q}\,/\,\mathfrak{p}}(\zeta_n) = \zeta_n^p \quad$ (as ζ_n^i are distinct in $\mathcal{O}_F\,/\,\mathfrak{q}$)
In particular $f_{\mathfrak{q}\,/\,\mathfrak{p}}$ = order of $\mathrm{Frob}_{\mathfrak{q}\,/\,\mathfrak{p}}$ =order of p in $(\mathbb{Z}\,/n\,\mathbb{Z})^\times$

2.3 Counting Primes

Lemma 2.10
F/K Galois extension of number fields

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

$$\mathfrak{p} \longleftrightarrow \{\text{primes above } \mathfrak{p} \text{ in } F\}$$

(ii) If $\mathfrak{q}$ is a prime of F above $\mathfrak{p}$, then

$$gD_{\mathfrak{q}} \mapsto g(\mathfrak{q}) \tag{2.16}$$

is a $\mathrm{Gal}(F/K)$-set isomorphism from $\{\text{primes above } \mathfrak{p}\}$ to $G/D_{\mathfrak{q}}$

(iii) $D_{g(\mathfrak{q})} = gD_{\mathfrak{q}}g^{-1} \quad$ and $\quad I_{g(\mathfrak{q})} = gI_{\mathfrak{q}}g^{-1}$

Proof
(1) follows from transitivity of $\mathrm{Gal}(F/K)$ of primes above $\mathfrak{p}$
(2),(3) is just elementary check $\square$

Corollary 2.11
F/K Galois, $L = K(\alpha)$ intermediate field. Then

$$\left\{ \begin{array}{c} \text{primes of } L \\ \text{above } \mathfrak{p} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} Gal(F/L)\text{-orbits on} \\ \text{primes of } F \text{ above } \mathfrak{p} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} H - D_{\mathfrak{q}} \text{ double cosets} \\ (H \backslash G / D_{\mathfrak{q}}) \end{array} \right\} \tag{2.17}$$

$$\mathfrak{s} \qquad \longmapsto \qquad \left(\begin{array}{c} \text{elements of } G \text{ that send} \\ \mathfrak{q} \text{ to a prime above } \mathfrak{s} \end{array} \right) \tag{2.18}$$

Note:

$$\begin{aligned} \{H - D \text{ double cosets}\} &= H\text{-orbits on } G/D & (2.19) \\ &= D\text{-orbits on } H\backslash G \qquad (D \text{ acts by } d(Hg) = Hgd^{-1}) & (2.20) \end{aligned}$$

Interpretation of the latter set:
H=Stabiliser of α in the action of G on the root of the minimal polynomial of α i.e. we want the $D_{\mathfrak{q}}$-orbits on the embeddings $L \hookrightarrow F$

Proposition 2.12
F/K Galois extension of number fields. $L = K(\alpha)$ an intermediate field, $G = \mathrm{Gal}(F/K), H = \mathrm{Gal}(F/L)$. Let $\mathfrak{p}$ be a prime of K, $\mathfrak{q}$ above p a prime at F
Consider the G-set (of size $[L : K]$)

$$X = H \setminus G \cong \{\text{embeddings} L \hookrightarrow F\} \cong \{\text{ roots of minimal polynomial of } \alpha\} \tag{2.21}$$

Then

$$\{\text{primes of } L \text{ above } \mathfrak{p}\} \overset{1-1}{\longleftrightarrow} D_{\mathfrak{q}\,/\,\mathfrak{p}}\text{-orbits on } X \qquad \text{with} \tag{2.22}$$

$$\begin{aligned} e_{\mathfrak{s}/\,\mathfrak{p}} f_{\mathfrak{s}/\,\mathfrak{p}} &= \text{size of the } D_{\mathfrak{q}}\text{-orbits} & (2.23) \\ e_{\mathfrak{s}/\,\mathfrak{p}} &= \text{size of any } I_{\mathfrak{q}}\text{-suborbit} & (2.24) \\ f_{\mathfrak{s}/\,\mathfrak{p}} &= \text{number of } I_{\mathfrak{q}}\text{suborbits} & (2.25) \end{aligned}$$

Explicitly

$$\mathfrak{s} \mapsto \text{Orbit of } g^{-1}(\alpha) \qquad \text{where } g(\mathfrak{q}) \text{ lies above } \mathfrak{s} \tag{2.26}$$

Proof
One-to-one correspondence:
This is the correspondence constructed in Corollary 2.11 and the note. Now,

$$\begin{aligned} \text{size of } D_{\mathfrak{q}}\text{-orbits of } g^{-1}(\alpha) &= \frac{|D_{\mathfrak{q}}|}{|\mathrm{Stab}_{D_{\mathfrak{q}}} g^{-1}(\alpha)|} = \frac{|D_{\mathfrak{q}}|}{|\mathrm{Stab}_{gD_{\mathfrak{q}}g^{-1}}(\alpha)|} & (2.27) \\ &= \frac{|D_{\mathfrak{q}}|}{|gD_{\mathfrak{q}}g^{-1} \cap H|} = \frac{|D_{\mathfrak{q}}|}{|D_{g(\mathfrak{q})/\mathfrak{s}}|} & (2.28) \\ &= \frac{e_{\mathfrak{q}\,/\,\mathfrak{p}} f_{\mathfrak{q}\,/\,\mathfrak{p}}}{e_{g(\mathfrak{q})/\mathfrak{s}} f_{g(\mathfrak{q})/\mathfrak{s}}} = \frac{e_{g(\mathfrak{q})/\,\mathfrak{p}} f_{g(\mathfrak{q})/\,\mathfrak{p}}}{e_{g(\mathfrak{q})/\mathfrak{s}} f_{g(\mathfrak{q})/\mathfrak{s}}} = e_{\mathfrak{s}/\,\mathfrak{p}} f_{\mathfrak{s}/\,\mathfrak{p}} & (2.29) \end{aligned}$$

Similarly,

$$\begin{aligned} \text{size of } I_{\mathfrak{q}}\text{-orbits} &= e_{\mathfrak{s}/\,\mathfrak{p}} \qquad \text{(note indepentdent of the suborbit)} & (2.30) \\ \Rightarrow \quad \text{number of } I_{\mathfrak{q}}\text{-suborbits} &= \frac{f_{\mathfrak{s}/\,\mathfrak{p}} e_{\mathfrak{s}/\,\mathfrak{p}}}{e_{\mathfrak{s}/\,\mathfrak{p}}} = f_{\mathfrak{s}/\,\mathfrak{p}} & (2.31) \end{aligned}$$

$\square$

Example:
$K = \mathbb{Q} \qquad F = \mathbb{Q}(\zeta_5, \sqrt[5]{2}) \qquad p = 73$
Fix $\mathfrak{r}, \mathfrak{q}$ primes above 73 in $\mathbb{Q}(\zeta_5)$ and F, respectively

- 73 is a generator of $(\mathbb{Z}/5\mathbb{Z})^\times \Rightarrow \mathfrak{r}$ has residue degree 4
- $\mathfrak{q}/p$ is unramified: otherwise $5|e_{\mathfrak{q}/73}$ which cannot happen as there is no ramification in $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$ (because $X^5 - 2$ has distinct roots mod 73)
  $\Rightarrow \quad e_{\mathfrak{q}/73} = 1 \quad f_{\mathfrak{q}/73} = 4$ or 20
  $\Rightarrow \quad I_{\mathfrak{q}} = \{1\} \quad D_{\mathfrak{q}} \cong C_4$ or C_{20}, but C_{20} is not a subgroup of $\mathrm{Gal}(F/\mathbb{Q})$
  $\Rightarrow \quad D_{\mathfrak{q}} \cong C_4$

Take $L = \mathbb{Q}(\sqrt[5]{2})$, $\mathrm{Gal}(F/\mathbb{Q})$ acts on $\sqrt[5]{2}, \zeta\sqrt[5]{2}, \zeta^3\sqrt[5]{2}$
WLOG $D_{\mathfrak{q}}$ fixes $\sqrt[5]{2}$ and cyclicly permutes the rest

$\Rightarrow$ 2 primes in L above 73; residue degree 1, 4; ramification degrees 1,1

2.4 Representations of the Decomposition Group

Convention for this section:
F/K Galois extension of number fields, $\mathfrak{p}$ a prime of K, $\mathfrak{q}$ lies above $\mathfrak{p}$
Write $D = D_{\mathfrak{q}/\mathfrak{p}}, I = I_{\mathfrak{q}/\mathfrak{p}}, \mathrm{Frob} = \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$
Notation:
If V is a representation of D, write V^I for the subspace of I-invariant vectors. As $I \trianglelefteq D$, this is a subrepresentation (Exercise: Check this)

Lemma 2.13
If V is an irreducible representation of D, then
either $V^I = 0$
or V is 1 dimensional, lifted from D/I (i.e. $D \to D/I \to \mathbb{C}$) (These kills I, and are determined by image of Frob)

Proof
V^I subrepresentation $\Rightarrow V^I = 0$ or $V^I = V$

If $V^I = V$, then the action of D factors through D/I. The latter is abelian (cyclic) $\Rightarrow V$ is 1 dimensional □

Remark. So representations of D look like $V = A \oplus B$ with
$A^I = 0 \quad , \quad B = V^I = \bigoplus$(1-dimensional representations of D/I)

Notation:
For V a D-representation, write

$$\Phi_{\mathfrak{q}/\mathfrak{p}}(V, t) = \det_{V^I}(t\mathrm{Id} - \mathrm{Frob}) \tag{2.32}$$
$$= \text{char polynomial of } \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \text{ on } V^I \tag{2.33}$$

Lemma 2.14
Let $\Psi : D \to D/I = \langle \text{Frob} \rangle \to \mathbb{C}^\times$ be a 1-dimensional representation of D, say $\Psi(\text{Frob}) = \zeta$
Then for a D-representation V

$$\langle \Psi, V \rangle = \langle \Psi, V^I \rangle = \text{multiplicity of } (t-\zeta) \text{ in } \Phi_{\mathfrak{q}/\mathfrak{p}}(t) \tag{2.34}$$

Proof
First equality is by definition Second equality is clear from previous remark. Example of this equality is $\Phi(\Psi, t) = t - \zeta$ □

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

Proposition 2.15
$K \subseteq L \subseteq F$ intermediate field
V a representation of $H = \text{Gal}(F/L)$, then

$$\Phi_{\mathfrak{q}/\mathfrak{p}}\left(\text{Res}^G_D \text{Ind}^G_H V, t\right) = \prod_{\mathfrak{s}} \Phi_{\mathfrak{q}/\mathfrak{s}}\left(\text{Res}^H_{D_{\mathfrak{p}_i/\mathfrak{s}}} V, t^{f_{\mathfrak{s}/\mathfrak{p}}}\right) \tag{2.35}$$

where $\mathfrak{s}$ runs over the primes of L above $\mathfrak{p}$, and $\mathfrak{q}_i$ lies above $\mathfrak{s}$ (a prime of F)

Proof
Will show that LHS and RHS have the same roots with same multiplicities. Note that the roots are $f_{\mathfrak{q}/\mathfrak{p}}$-th roots of unity
Let S be such a root, and set $\Psi : D \to D/I \to \mathbb{C}^\times$ with $\Psi(\text{Frob}) = \zeta$, then

$$\begin{aligned}
\begin{array}{c}\text{multiplicity of}\\ t-\zeta \text{ in LHS}\end{array} &= \langle \Psi, \text{Res}^G_D \text{Ind}^G_H V \rangle \qquad \text{by Lemma 2.14} && (2.36)\\
&= \sum_{x \in H\backslash G/D} \langle \Psi, \text{Ind}^D_{x^{-1}Hx\cap D} \text{Res}^{x^{-1}Hx}_{x^{-1}Hx\cap D} V^x \rangle && (2.37)\\
&= \sum_{\mathfrak{s}} \langle \Psi^{x^{-1}}, \text{Ind}^{D_{\mathfrak{q}_i/\mathfrak{p}}}_{D_{\mathfrak{q}_i/\mathfrak{s}}} \text{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V \rangle \qquad \text{by Lemma 2.10(3)} && (2.38)\\
&= \sum_{\mathfrak{s}} \langle \text{Res}_{D_{\mathfrak{q}_i/\mathfrak{s}}} \Psi^{x^{-1}}, \text{Res}_{D_{\mathfrak{q}_i/\mathfrak{s}}} V \rangle \qquad \text{by Frobenius Reciprocity} && (2.39)\\
&= \sum_{\mathfrak{s}} \text{multiplicity of } \left(t - \zeta^{f_{\mathfrak{s}/\mathfrak{p}}}\right) \quad \text{in } \Phi_{\mathfrak{q}_i/\mathfrak{s}}\left(\text{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V, t\right) && (2.40)\\
&= \sum_{\mathfrak{s}} \text{multiplicity of } (t-\zeta) \qquad \text{in } \Phi_{\mathfrak{q}_i/\mathfrak{s}}\left(\text{Res}^H_{D_{\mathfrak{q}_i/\mathfrak{s}}} V, t^{f_{\mathfrak{s}/\mathfrak{p}}}\right) && (2.41)
\end{aligned}$$

□

Corollary 2.16
Take $\Psi_n : D \to D/I \to \mathbb{C}^\times$ which maps Frob to ζ a primitive n-th root of unity $(n|f_{\mathfrak{q}\,/\,\mathfrak{p}})$, then

$$\begin{array}{c}\text{number of primes } \mathfrak{s} \text{ of } L \\ \text{above } \mathfrak{p} \text{ with } n|f_{\mathfrak{s}/\,\mathfrak{p}}\end{array} = \langle \Psi_n, \mathrm{Res}_D \underbrace{\mathrm{Ind}_H^G}_{\mathbb{C}[G/H]} \mathbb{1}\rangle \tag{2.42}$$

Proof

$$\begin{aligned}
\langle \Psi_n, \mathrm{Res}_D \mathrm{Ind}_H^G \mathbb{1}\rangle &= \begin{array}{c}\text{multiplicity of } t-\zeta \\ \text{in } \Phi_{\mathfrak{q}\,/\,\mathfrak{p}}(\mathrm{Res}\,\mathrm{Ind}\,\mathbb{1}, t)\end{array} && \text{by Lemma 2.14} && (2.43)\\
&= \prod_{\mathfrak{s}} \Phi_{\mathfrak{q}_i\,/\mathfrak{s}}\left(\mathbb{1}, t^{f_{\mathfrak{s}/\,\mathfrak{p}}}\right) && \text{by Proposition 2.15} && (2.44)\\
&= \begin{array}{c}\text{multiplicity of } \zeta \\ \text{in } \prod_{\mathfrak{s}}\left(t^{f_{\mathfrak{s}}/\,\mathfrak{p}} - 1\right)\end{array} && && (2.45)\\
&= \begin{array}{c}\text{number of prime } \mathfrak{s} \\ \text{with } n|f_{\mathfrak{s}/\,\mathfrak{p}}\end{array} && && (2.46)
\end{aligned}$$

□

Exercise: Deduce Corollary 2.16 from Proposition 2.12

3 L-series

Aim/Motivation:

(i) If $(a, n) = 1$, then $\exists$ infinitely many primes $p \cong a \mod n$

(ii) If $f(X) \in \mathbb{Z}[X]$, monic, and suppose that $f(X) \mod p$ has a root $\forall$ prime $p \Rightarrow f(X)$ reducible

Definition 3.1
An (ordinary) Dirichlet series is a series

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

(Warning/Convention: The complex variable is $s = \sigma + it$, NOT $z = x + iy$)

3.1 Convergence Properties

Lemma 3.2 (Abel's Lemma)

$$\sum_{n=N}^{M} a_n b_n = \sum_{n=N}^{M-1}\left(\sum_{k=N}^{n} a_k\right)(b_n - b_{n+1}) + \left(\sum_{k=N}^{M} a_k\right) b_M \tag{3.1}$$

Proof
Elementary rearrangement □

(c.f. $\int u dv = [uv] - \int v du, \quad a \leftrightarrow dv, b \leftrightarrow du$)

Proposition 3.3
Let

$$f(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s} \qquad \text{for } \lambda_n \to \infty \tag{3.2}$$

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 $\mathrm{Re}(s) > 0$ to an analytic function

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

Note: Dirichlet series are the case $\lambda_n = \log n$

Proof
(i) $\Rightarrow$ (ii):
Change variables $s' = s - s_0$, $a'_n = a_n e^{-\lambda_n s_0}$
The new series converges at 0, so must have $\sum_N^M a'_n$ bounded. Invoke (i)

(ii): We show uniform convergence on $-A < \arg(s) < A, \mathrm{Re}(s) > \delta$ with $0 < A < \pi/2$. This will suffice as the uniform limit of analytic functions is analytic
Let $\epsilon > 0$. Find N_0 s.t. for $n \geq N_0$ have $\left|e^{-\lambda_n s}\right| < \epsilon$ in this domain.
Now compute for $N, M \geq N_0$,

$$\begin{aligned}
\left|\sum_{n=N}^{M} a_n e^{-\lambda_n s}\right| &= \left|\sum_{n=N}^{M-1}\left(\sum_{k=N}^{n} a_k\right)\left(e^{-\lambda_n s} - e^{-\lambda_{n+1} s}\right) + \left(\sum_{N}^{M} a_k\right) e^{-\lambda_M s}\right| \qquad (3.3)\\
& \quad \text{(by Abel's Lemma 3.2)}\\
&\leq B \sum_{n=N}^{M-1} \left|e^{-\lambda_n s} - e^{-\lambda_{n+1} s}\right| + B\epsilon \qquad (3.4)
\end{aligned}$$

where B is the bound on the partial sums $\sum a_k$
Observe that

$$\begin{aligned}
\left|e^{-\alpha s} - e^{-\beta s}\right| &= \left|s \int_\alpha^\beta e^{-xs} dx\right|\\
&= |s| \int_\alpha^\beta e^{-x\sigma} dx \quad (\sigma = \mathrm{Re}(s))\\
&= \frac{|s|}{\sigma}\left(e^{-\alpha\sigma} - e^{-\beta\sigma}\right) \qquad (3.5)
\end{aligned}$$

Therefore,

$$\begin{aligned}
\left|\sum_{n=N}^{M} a_n e^{-\lambda_n s}\right| &\leq B\frac{|s|}{\sigma} \sum_{n=N}^{M-1}\left(e^{-\lambda_n \sigma} - e^{-\lambda_{n+1}\sigma}\right) + B\epsilon \qquad (3.6)\\
&= B\frac{|s|}{\sigma}\left(e^{-\lambda_N \sigma} - e^{-\lambda_M \sigma}\right) + B\epsilon \qquad (3.7)\\
&\leq \epsilon\left(B\frac{|s|}{\sigma} + B\right) \leq \epsilon(Bk + B) \quad \text{where } \frac{|s|}{\sigma} \leq k \text{ in our domain} \qquad (3.8)
\end{aligned}$$

This is uniform convergence ☐

Proposition 3.4
Let $f(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$ for $\lambda_n \to \infty$ increasing sequence of positive real numbers. Suppose

(i) $0 \leq a_n \in \mathbb{R}$

(ii) $f(s)$ converges on $\mathrm{Re}(s) > R \in \mathbb{R}$ (and hence analytic there)

(iii) It has an analytic continuation to a neighbourhood of $s = R$

Then $f(s)$ converges on $\mathrm{Re}(s) > R - \epsilon$ for some $\epsilon > 0$

Proof
Again, we may assume $R = 0$
f analytic on $\mathrm{Re}(s) > 0$ and on $|s| < \delta$
$\Rightarrow$ f analytic on $|s - 1| \leq 1 + \epsilon$
The Taylor series of f around $s = 1$ converges on all of $|s-1| \leq 1+\epsilon$. In particular

$$f(-\epsilon) = \sum_{k=0}^{\infty} \frac{1}{k!}(-1)^k(1+\epsilon)^k f^{(k)}(1) \qquad \text{converges} \tag{3.9}$$

For $\mathrm{Re}(s) > 0$

$$f^{(k)}(s) = \sum_{n=1}^{\infty} a_n(-\lambda_n)^k e^{-\lambda_n s} \qquad \begin{pmatrix}\text{term-by-term differentiation okay} \\ \text{by locally uniform convergence}\end{pmatrix} \tag{3.10}$$

$$(-1)^k f^{(k)}(1) = \sum_{n=1}^{\infty} a_n \lambda_n^k e^{-\lambda_n s} \qquad \text{a convergent series with positive terms} \tag{3.11}$$

Observe:

$$f(-\epsilon) = \sum_{k=0}^{\infty} \frac{1}{k!}(1+\epsilon)^k \sum_{n=1}^{\infty} a_n \lambda_n^k e^{-\lambda_n s} \tag{3.12}$$

$$= \sum_{k,n} a_n \lambda_n^k e^{-\lambda_n s} \frac{1}{k!}(1+\epsilon)^k \qquad \begin{pmatrix}\text{order does not matter} \\ \text{as all terms positive}\end{pmatrix} \tag{3.13}$$

$$= \sum_{n=1}^{\infty} a_n e^{-\lambda_n} e^{\lambda_n(1+\epsilon)} \tag{3.14}$$

$$= \sum_{n=1}^{\infty} a_n e^{\lambda_n \epsilon} \qquad \text{is a convergent series} \tag{3.15}$$

Therefore, series for f converges at $s = -\epsilon$, and hence, by Proposition 3.3, on $\mathrm{Re}(s) > -\epsilon$ $\square$

Exercise:
Show that, if $\sum a_n e^{-\lambda_n s}$ and $\sum b_n e^{-\lambda_n s}$ converges on $\mathrm{Re}(s) > \sigma_0$ to the same function $f(s)$, then $a_n = b_n \; \forall n$

Theorem 3.5

(i) If a_n are bounded, then $\sum_{n=1}^{\infty} a_n n^{-s}$ converges absolutely on $\mathrm{Re}(s) > 1$ to an analytic fucntion

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

Proof

(i) $\sum \frac{1}{n^x}$ converges for $x > 1$ real. Analyticity from Proposition 3.3

(ii) by Proposition 3.3

□

3.2 Dirichlet L-functions

Definition 3.6
Let $N \geq 1$ be an integer and

$$\psi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^t imes \tag{3.16}$$

a group homomorphism. Extend ψ to all of $\mathbb{Z}$ by

$$\psi(n) = \begin{cases} \psi(n \mod N) & \text{if } (n, N) = 1 \\ 0 & \text{otherwise} \end{cases} \tag{3.17}$$

Such a function is called Dirichlet character modulo N
Its L-series (or L-function) is

$$L_N(\psi, s) = \sum_{n=1}^{\infty} \psi(n), n^{-s} \tag{3.18}$$

Remark. $\psi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is often called Dirichlet character
Warning: Note that ψ is just a 1-dimensional representation. Number theorists often have the (bad) habit of referring to 1-dimensional representations as characters

Lemma 3.7
Let ψ be a Dirichlet character modulo N

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

(ii) $\psi(ab) = \psi(a)\psi(b)$ (ψ is strictly multiplicative)

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

$$L_N(\psi, s) = \prod_{p \text{ prime}} \frac{1}{1 - \psi(p)p^{-s}} \tag{3.19}$$

(This expression is called the Euler product for ψ)

Proof

(i) Clear

(ii) Clear

(iii) Coefficients, $\psi(n)$, of the L-series are bounded, so absolute convergence follows from Theorem 3.5(i). For $\mathrm{Re}(s) > 1$

$$\sum \psi(n)n^{-s} = \prod_{p \text{ prime}} \left(1 + \psi(p)p^{-s} + \psi(p)^2 p^{-2s} + \psi(p)^3 p^{-3s} + \cdots\right) \quad \text{by (ii) and absolute convergence} \tag{3.20}$$

$$= \prod_{p \text{ prime}} \frac{1}{1 - \psi(p)p^{-s}} \qquad \text{Geometric series} \tag{3.21}$$

□

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

$$L_{10}(\psi, s) = 1 + \frac{i}{3^s} - \frac{i}{7^s} - \frac{1}{9^s} + \frac{1}{11^s} + \frac{1}{13^s} - \frac{1}{17^s} - \frac{1}{19^s} + \cdots \tag{3.22}$$

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

$$L_N(\psi, s) = \zeta(s) \prod_{\text{prime } p|N} \left(1 - p^{-s}\right) \tag{3.23}$$

($\zeta(s)$ =Riemann ζ-function, both sides are $\prod_{p\nmid N} 1/(1-p^{-s})$)

Theorem 3.8
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 analytic continuation to $\mathrm{Re}(s) > 0$ except for a simple pole at $s = 1$

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

Proof

(i) Follows from last remark and that $\zeta(s)$ has an analytic continuation to $\mathrm{Re}(s) > 0$ with a simple pole at $s = 1$ (c.f. Part II Number Theory)

(ii)

$$\begin{aligned} \sum_{n=A}^{A+N+1} \psi(n) &= \sum_{n\in(\mathbb{Z}/N\mathbb{Z})^\times} \psi(n) && (3.24)\\ &= \langle \psi, \mathbb{1} \rangle \qquad \text{(representation of } (\mathbb{Z}/N\mathbb{Z})^\times) && (3.25)\\ &= 0 \qquad \text{as } \psi \neq \mathbb{1} && (3.26) \end{aligned}$$

So the sums $\sum_{n=A}^{B} \psi(n)$ are bounded, and result follows from Theorem 3.5(ii)

□

Theorem 3.9
Let ψ be a non-trivial Dirichlet character modulo N.
Then $L_N(\psi, 1) \neq 0$

Proof
Let

$$\zeta_N(s) = \prod_{\chi(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} L_N(\chi, s) \tag{3.27}$$

Suppose $L_N(psi, 1) = 0$. Then $\zeta_N(s)$ has an analytic continuation to $\mathrm{Re}(s) > 0$ by Theorem 3.8, the pole from $L_N(\mathbb{1}, s)$ having been killed by the zero of $L_N(\psi, s)$
On $\mathrm{Re}(s) > 1$, $\zeta_N(s)$ has the absolute convergence Euler product

$$\zeta_N(s) = \prod_\chi \prod_p \frac{1}{1 - \chi(p)p^{-s}} = \prod_p \prod_\chi \frac{1}{1 - \chi(p)p^{-s}} \tag{3.28}$$

Now,

$$\prod_{\chi}(1-\chi(p)T)=\left(1-T^{f_p}\right)^{\phi(N)/f_p} \tag{3.29}$$

where f_p=order of p modulo N, and ϕ is the Euler-totient function.
Indeed, the $\chi(p)$ are f_p-th roots of unity, each occuring $\phi(N)/f_p$ times and $\prod_{i=0}^{f_p-1}\left(1-\zeta_{f_p}^i T\right)=1-T^{f_p}$
So on $\mathrm{Re}(s)>1$, $\zeta_n(s)$ has a Dirichlet series give by

$$\zeta_N(s)=\prod p\nmid N\left(1+p^{-f_ps}+p^{-2f_ps}+\cdots\right)^{\phi(N)/f_p} \tag{3.30}$$

By Proposition 3.4, as $\zeta_N(s)$ is assumed analytic on $\mathrm{Re}(s)>0$ and this series has positive coefficients, the series must converge on $\mathrm{Re}(s)>0$. But (for $s>0$ real) it dominates

$$\prod_{p\nmid N}\left(1+p^{-f_ps}+p^{-2f_ps}+\cdots\right)=L_N(\mathbb{1},\phi(N)s) \tag{3.31}$$

which diverges when $s\to 1/\phi(N)$ # □

Want:

$$\sum_{p\cong a \mod N} p^{-s}\to\infty \quad \text{as} \quad s\to 1 \tag{3.32}$$

3.3 Primes in Arithmetic Progressiona

Proposition 3.10
Let ψ be Dirichlet character mod N

(i) The Dirichlet series $\displaystyle\sum_{p \text{ primes},n\geq 1}\frac{\psi(p)^n}{n}p^{-ns}$ converges absolutely on $\mathrm{Re}(s)>1$ to an analytic function and defines (a branch of) $\log L_N(\psi,s)$ there

(ii) If ψ is non-trivial then $\displaystyle\sum_{p>n}\frac{\psi(p)^n}{n}p^{-ns}$ is bounded as $s\to 1$
If $\psi=\mathbb{1}$ then $\displaystyle\sum_{p>n}\frac{psi(p)^n}{n}p^{-ns}\sim\log\frac{1}{s-1}$ as $s\to 1$

Proof

(i) The series has bounded coefficients so converges absolutely on $\mathrm{Re}(s)>1$ to an analytic function (Theorem 3.5(i)). Then

$$\begin{aligned}
\sum_{p>n}\frac{psi(p)^n}{n}p^{-ns} &= \sum_p \psi(p)p^{-s}=\frac{\psi(p)^2p^{-2s}}{2}+\cdots && (3.33)\\
&= \sum_p\log\frac{1}{1-\psi(p)p^{-s}} && (3.34)\\
&= \log\prod_p\frac{1}{1-\psi(p)p^{-s}} \qquad \text{continuity of log and local uniform converges of } L_N(\psi,s) && (3.35)\\
&= \log L_N(\psi,s) && (3.36)
\end{aligned}$$

Note, in equation 3.34, the branch we took is

$$\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots \qquad \text{for } x \text{ small} \tag{3.37}$$

And at the end, it is possible that we will get a different branch of log

(ii) By Theorem 3.8 if ψ is non-trivial the $L_N(\psi, s)$ converges to a nonzero value as $s \to 1$, so its logarithm is bounded near $s = 1$
$L_N(\psi, s)$ have a simple pole at $s = 1 \Rightarrow sim\frac{\lambda}{s-1}$

$$\log L_N(\mathbb{1}, s) \sim \log \frac{1}{s-1} \quad \text{as } s \to 1 \tag{3.38}$$

□

Corollary 3.11
If ψ nontrivial then $\sum_{p \text{ prime}} \psi(p)p^{-s}$ is bounded as $s \to 1$.
If $\psi = \mathbb{1}$ then $\sum_{p \text{ prime}} \psi(p)p^{-s} = \sum_{p \nmid N} p^{-s} \sim \log \frac{1}{s-1}$ as $s \to 1$

Proof

$$\sum_p \psi(p)p^{-s} = \log L_N(\psi, s) - \sum_{p, n \geq 2} \frac{\psi(p)^n}{n} p^{-ns} \tag{3.39}$$

So sufficient to prove that, the last term is bounded on $\mathrm{Re}(s) > 1$. But there

$$\begin{aligned}
\left| \sum_{p,n\geq 2} \frac{\psi(p)^n}{n} p^{-ns} \right| &\leq \sum_{p,n\geq 2} \frac{1}{|p^s|^n} && (3.40)\\
&= \sum_p \frac{1}{|p^s|^2(|p^s|-1)} \quad \text{Geometric series} && (3.41)\\
&\leq \sum_p \frac{1}{p(p-1)} \quad \mathrm{Re}(s) > 1 && (3.42)\\
&\leq \sum_n \frac{1}{n^2} < \infty && (3.43)
\end{aligned}$$

□

Theorem 3.12 (Dirichlet's Theorem on Primes in Arithmetic Progressions)
Let a, N be coprime integers. Then there are infinitely many primes p with $p \cong a \mod N$
Moreover, if P_a is the set of these primes, then

$$\sum_{p \in P_a} \frac{1}{p^s} \sim \frac{1}{\phi(N)} \log \frac{1}{s-1} \quad \text{as } s \to 1 \tag{3.44}$$

Proof
Second statement ;$\Rightarrow$ First statement. So we will prove the second statement.

Consider the (class) function

$$\begin{aligned}
C_a : (\mathbb{Z}/n\,\mathbb{Z})^\times &\to \mathbb{C} && (3.45)\\
C_a(n) &= \begin{cases} 1 & \text{if } n \cong a \\ 0 & \text{otherwise} \end{cases} && (3.46)
\end{aligned}$$

Then

$$\langle C_a, \chi \langle = \frac{1}{\phi(N)} \sum_{n \in (\mathbb{Z}/n\mathbb{Z})^\times} C_a(n)\overline{chi}(n) = \frac{1}{\phi(N)}\overline{\chi(a)} \tag{3.47}$$

$$\Rightarrow \qquad C_a = \sum_{\chi:(\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times} \frac{\overline{\chi(a)}}{\phi(N)}\chi \tag{3.48}$$

Hence

$$\sum_{p \in P_a} \frac{1}{p^s} = \sum_{p \text{ prime}} C_a(p)p^{-s} = \sum_{\chi} \left(\frac{\overline{\chi(a)}}{\phi(N)} \sum_p \frac{\chi(p)}{p^s} \right) \tag{3.49}$$

Each term on RHS is bounded as $s \to 1$ except $\chi = \mathbb{1}$ (by Corollary 3.11) and

$$\frac{\mathbb{1}(a)}{\phi(N)} \sum_p \frac{\mathbb{1}(p)}{p^s} = \frac{1}{\phi(N)} \sum_p \frac{1}{p^s} \sim \frac{1}{\phi(N)} \log \frac{1}{s-1} \tag{3.50}$$

as $s \to 1$ $\square$

Summary:

$$\sum_{p \cong a \mod N} p^{-s} = \begin{array}{l} \text{linear combination of } \sum_p \chi(p)p^{-s} \\ \text{with } \frac{1}{\phi(N)} \text{ copies of } \mathbb{1} \end{array} \tag{3.51}$$

$$\text{each } \sum \chi(p)p^{-s} = \approx \log L_N(\chi, s) \tag{3.52}$$

and these are bounded for $\chi \neq \mathbb{1}$ ($L_N(\chi,1) \neq 0, \infty$) and $\sim \log 1s - 1$ for $\chi = \mathbb{1}$

3.4 Dirichlet Characters, Alternative view

We want to pass Dirichlet from $\mathbb{Z}, \mathbb{Q}$ to $\mathcal{O}_K, K$ and look at mod I (correspond to APs)

Note:

$$(\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \tag{3.53}$$

$$a \mapsto \sigma_a \quad \text{with } \sigma_a(\zeta_N) = \zeta_N^a \tag{3.54}$$

$$p \mapsto \sigma_p \quad \text{with } \sigma_p(\zeta_N) = \zeta_N^p \tag{3.55}$$

If $\mathfrak{q} \subseteq \mathbb{Q}(\zeta_N)$ above $p \nmid N$, then $\sigma_p = \mathrm{Frob}_{\mathfrak{q}/p}$

$$\Rightarrow \qquad \frac{1}{1 - \psi(p)p^{-s}} \longleftrightarrow \frac{1}{1 - \psi(\mathrm{Frob}_p)p^{-s}} \tag{3.56}$$

($\mathrm{Frob}_p = \mathrm{Frob}_{\mathfrak{q}/p}$ and $\mathfrak{q}\,|p$)

Theorem 3.13 (Hecke, 1920, Class Field Theory related)
Let F/K be a Galois extension of number fields with $\mathrm{Gal}(F/K)$ abelian, and $\psi : \mathrm{Gal}(F/K) \to \mathbb{C}^\times$ a homomorphism. Then

$$L_*(\psi, s) = \prod_{\substack{\mathfrak{p} \text{ prime in } K \\ \text{unram. in } F/K}} \frac{1}{1 - \psi(\mathrm{Frob}_\mathfrak{p})N(\mathfrak{p})^{-s}} \tag{3.57}$$

has an analytic continuation to $\mathbb{C}$, except for a simple pole at $s = 1$ when $\psi = \mathbb{1}$ (Note:
$\mathfrak{p}$ unramified $\Rightarrow$ Inertia group=1, and
$\mathrm{Frob}_\mathfrak{p} = \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ independent of $\mathfrak{q}$ as $\mathrm{Gal}(F/K)$ is abelian)

Proof
Beyond syllabus $\square$

Remark. When $K = \mathbb{Q}$, $F = \mathbb{Q}(\zeta_N)$, this recovers Theorem 3.8

3.5 Artin L-functions

AIM: Prove $f(X)$ has a root mod all prime $\Rightarrow$ $f(X)$ reducible
Recall (Noatation):
For $I \leq D$ finite groups and ρ a D-representation

- $\rho^I = I$-invariant vectors of $\rho = \{v \in \rho | gv = v \ \forall g \in I\}$
- If $I \lhd D$ then ρ^I is a subrepresentation
  $(v \in \rho^I, g \in D, i \in I$
  $\Rightarrow \quad i(gv) = g(i'v) = gv$ (for some $i' \in I$)
  $\Rightarrow \quad gv \in \rho^I)$
- If $\lambda \in \mathbb{C}, g_i \in D$, write $\det(\sum \lambda_i g_i | \rho)$ for $\det_\rho(\sum \lambda_i g_i)$
  equivalent viewing ρ as $\rho : D \to GL_n(\mathbb{C})$
  $\det(\lambda_i g_i|\rho) = \det(\sum \lambda_i \rho(g_i))$
  e.g. charactieristic polynomial of $g \in D$ is $\det(t - g|\rho)$

Definition 3.14
Let F/K be Galois extension of number fields and ρ a $\mathrm{Gal}(F/K)-$representation.
Let $\mathfrak{p}$ be a prime in K. Choose a prime in F above $\mathfrak{p}$ and an element $\mathrm{Frob}_\mathfrak{p} \in D_{\mathfrak{q}/\mathfrak{p}}$ which maps to $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in D_\mathfrak{q}/I_\mathfrak{q}$, i.e. that acts as Frobenius on the residue field at $\mathfrak{q}$
Then the local polynomial of ρ at $\mathfrak{p}$ is

$$P_\mathfrak{p}(F/K, \rho, T) = P_\mathfrak{p}(\rho, T) = \det(1 - \mathrm{Frob}_\mathfrak{p} T | \rho^{I_\mathfrak{p}}) \tag{3.58}$$

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

Remark. This is essentially the characteristic polynomial of $\mathrm{Frob}_\mathfrak{p}$ on ρ, $\Phi_{\mathfrak{q}/\mathfrak{p}}(\rho, T)$
If $P_\mathfrak{p}(\rho, T) = 1 + a_1 T + a_2 T^2 + \cdots + a_n T^n$
then $\Phi_{\mathfrak{q}/\mathfrak{p}}(\rho, T) = T^n + a1T^{n-1} + a_2 T^{n-2} + \cdots + a_n$

Lemma 3.15
$P_\mathfrak{p}(\rho, T)$ independent of the choice of $\mathfrak{q}$ and of the choice of $\mathrm{Frob}_\mathfrak{p}$

Proof
For fixed $\mathfrak{q}$, independence of choice of $\mathrm{Frob}_\mathfrak{p}$ is clear.
Two choices differ by some $i \in I$ which acts as identity on ρ^I
If $\mathfrak{q}'$ is a different prime over $\mathfrak{p}$, write $\mathfrak{q}' = g(\mathfrak{q})$ for some $g \in \mathrm{Gal}(F/K)$ and observe $\mathrm{Frob}'_\mathfrak{p} = g \,\mathrm{Frob}_\mathfrak{p}\, g^{-1}$ is a lift of Frobenius for $\mathfrak{q}'/\mathfrak{p}$.
The equivalence of $\mathrm{Frob}'_\mathfrak{p}$ on $\rho^{I_{\mathfrak{q}'/\mathfrak{p}}} = \rho^{g I_\mathfrak{p} g^{-1}}$ are the same as of $\mathrm{Frob}_\mathfrak{p}$ on $\rho^{I_\mathfrak{p}}$
Hence, their characteristic polynomials agree
$\Rightarrow \quad P_\mathfrak{p}(\rho, T)$ is independent of choice of $\mathfrak{q}$ $\square$

Definition 3.16
Let F/K be a Galois extension of number fields. ρ a representation of $\mathrm{Gal}(F/K)$
The Artin L-function of ρ is defined by the Euler product

$$L(F/K, \rho, s) = L(\rho, s) = \prod_{\mathfrak{p} \text{ prime of } K} \frac{1}{P_\mathfrak{p}(\rho, N(\mathfrak{p})^{-s})} \tag{3.59}$$

The polynomial $P_{\mathfrak{p}}(\rho, T)$ has the form $1 - (aT + bT^2 + \cdots)$
so we can write (ignoring convergence)

$$\frac{1}{P_{\mathfrak{p}}(\rho, T)} - 1 + (aT + bT^2 + \cdots) + (aT + bT^2 + \cdots)^2 + \cdots \tag{3.60}$$

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

$$L(\rho, s) = \sum_{\substack{\mathfrak{n} \text{ non-zero} \\ \text{ideal in } \mathcal{O}_K}} a_{\mathfrak{n}} N(\mathfrak{n})^{-s} = \left[\prod_{\mathfrak{p}} (1 + a_{\mathfrak{p}} N(\mathfrak{p})^{-s} + a_{\mathfrak{p}^2} N(\mathfrak{p})^{-2s} + \cdots)\right] \tag{3.61}$$

for some $a_{\mathfrak{n}} \in \mathbb{C}$
Note that the grouping ideal with equal norm yields an expression for $L(\rho, s)$ as an ordinary Dirichlet series

Lemma 3.17
The L-series expression for $L(\rho, s)$ agrees with the Euler product on $\mathrm{Re}(s) > 1$ where they converge absolutely to an analytic function

Proof
It suffices to prove that

$$\prod_{\mathfrak{p} \text{ prime of } \mathcal{O}_K} (1 + a_{\mathfrak{p}} N(\mathfrak{p})^{-s} + a_{\mathfrak{p}^2} N(\mathfrak{p})^{-2s} + \cdots) \tag{3.62}$$

converges absolutely on $\mathrm{Re}(s) > 1$, this justifies rearrangement of terms and the Dirichlet series expression for $L(\rho, s)$ then proves analyticity (Proposition 3.3)
The polynomial $P_{\mathfrak{p}}(\rho, T)$ factorises over $\mathbb{C}$ as

$$P_{\mathfrak{p}}(\rho, T) = (1 - \lambda_1 T)(1 - \lambda_2 T) \cdots (1 - \lambda_k T) \tag{3.63}$$

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

$$\frac{1}{P_{\mathfrak{p}}(\rho, T)} = \frac{1}{\prod(1 - \lambda_i T)} = 1 + a_{\mathfrak{p}} T + a_{\mathfrak{p}^2} T^2 + \cdots \tag{3.64}$$

are bounded in absolute value by those of $\dfrac{1}{(1-T)^{\dim \rho}} = (1 + T + T^2 + \cdots)^{\dim \rho}$
Hence,

$$\begin{aligned}
\prod_{\mathfrak{p}} \sum_n |a_{\mathfrak{p}^n}||N(\mathfrak{p})^{-ns}| &\leq \prod_{\mathfrak{p}} \frac{1}{(1 - |N(\mathfrak{p})^{-s}|)^{\dim \rho}} && (3.65) \\
&\leq \prod_{\mathfrak{p}} \frac{1}{(1 - |p^{-s}|)^{\dim \rho}} \quad (p \text{ a rational prime below } \mathfrak{p}) && (3.66) \\
&\leq \prod_{p \text{ prime}} \left(\frac{1}{1 - |p^{-s}|}\right)^{\dim \rho [K:\mathbb{Q}]} && (3.67) \\
&= \zeta(\sigma)^{\dim \rho [K:\mathbb{Q}]} \quad \text{where } \sigma = \mathrm{Re}(s) && (3.68) \\
&< \infty && (3.69)
\end{aligned}$$

□

Example:

(i) $K = \mathbb{Q}$ $\quad$ F arbitrary $\quad$ $\rho = \mathbb{1}$
For a prime p, $\rho^{I_\mathfrak{p}} = \rho$ and $\mathrm{Frob}_\mathfrak{p}$ acts as identity so $P_\mathfrak{p}(\rho, T) = 1 - T$

$$\Rightarrow \qquad L(F/\mathbb{Q}, \mathbb{1}, s) = \prod_p \frac{1}{1 - p^{-s}} = \zeta(s) \tag{3.70}$$

(Note that this does not depends on F, and all factors are in place)

(ii) K, F are arbitrary, $\rho = \mathbb{1}$

$$L(F/K, \mathbb{1}, s) = \prod_\mathfrak{p} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \zeta_K(s) \tag{3.71}$$

This is the Dedekind ζ-function of K

(iii) $K = \mathbb{Q}, F = \mathbb{Q}(\zeta_N), \rho$ 1-dimensional representation of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$
Set

$$\psi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times \tag{3.72}$$
$$\psi(n) = \rho(\sigma_n) \qquad \text{where } \sigma_n(\zeta_N) = \zeta_N^n \tag{3.73}$$

$$\begin{aligned} \Rightarrow \qquad L(\rho, s) &= \prod_{p:\rho(I_p)=1} \frac{1}{1 - \rho(\mathrm{Frob}_p)p^{-s}} && (3.74) \\ &= \prod_{p:\rho(I_p)=1} \frac{1}{1 - \psi(p)p^{-s}} && (3.75) \\ &= L_N(\psi, s) \prod_{p|N,\rho(I_p)=1} \frac{1}{1 - \rho(\mathrm{Frob}_p)p^{-s}} && (3.76) \end{aligned}$$

for example, if ρ is faithful then $L(\rho, s) = L_N(\psi, s)$

Proposition 3.18
F/K Galois extension of number fields, ρ a $\mathrm{Gal}(F/K)$-representation

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

$$L(\rho \oplus \rho', s) = L(\rho, s)L(\rho', s) \tag{3.77}$$

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

$$L(F/K, \rho, s) = L(F^N/K, \rho'', s) \tag{3.78}$$

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

$$L(F/K, \rho, s) = L(F/F^H, \rho''', s) \tag{3.79}$$

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

(i) Clear. (Note $(\rho \oplus \rho')^{I_p} = \rho^{I_p} \oplus \rho'^{I_p}$)

(ii) Straight from the definitions (Note Frobenius for F/K projects to Frobenius for F^N/K and similarly for inertia)

(iii) We have already proved this in Proposition 2.15 (for characteristic polynomial Φ) and the remark under Definition 3.14 (to get local polynomials)

$\square$

Theorem 3.19
(This theorem rephrase Theorem 3.13) F/K Galois extension of number fields, ρ a 1-dimensional representation of $\mathrm{Gal}(F/K)$
Then $L(\rho, s)$ has analytic continuation of $\mathbb{C}$, except for a simple pole at $s = 1$ if $\rho = \mathbb{1}$

Proof
By Proposition 3.18(ii), we may assume that ρ is faithful

$$\Rightarrow \qquad \rho^{I_\mathfrak{p}} = \begin{cases} \rho & \mathfrak{p} \text{ unramified in } F/K \\ 0 & \mathfrak{p} \text{ ramified} \end{cases} \tag{3.80}$$

Then by Theorem 3.13:

$$L(\rho, s) = \prod_{\substack{\mathfrak{p}\,\text{unram} \\ \text{in } F/K}} \frac{1}{1 - \rho(\mathrm{Frob}_\mathfrak{p}) N(\mathfrak{p})^{-s}} \tag{3.81}$$

$\square$

Theorem 3.20 (Artin)
Let G be a finite group, ρ a G-representation.
There are cyclic subgroups $H_i, H'_j \leq G$ and 1-dimensional representations ψ_i, ψ'_j of H_i, H'_j respectively, s.t.

$$\rho^{\oplus n} \oplus \left(\bigoplus \mathrm{Ind}_{H_i}^G \psi_i \right) \cong \bigoplus_j \mathrm{Ind}_{H_j}^G \psi'_j \tag{3.82}$$

for some $n \geq 1$
Moreover, if $\langle \rho, \mathbb{1} \rangle = 0$ then all ψ_i, ψ'_j can be taken to be non-trivial

(see handout for proof, non-examinable)

Corollary 3.21 (Artin)
F/K Galois extension of number fields, ρ a $\mathrm{Gal}(F/K)$-representation.
Then $\exists n \geq 1$ s.t. $L(\rho, s)^n$ admits a meromorphic continuation to $\mathbb{C}$
(and analytic at $s = 1$ if $\langle \rho, \mathbb{1} \rangle = 0$)

Proof
Combine Theorem 3.20 with Proposition 3.18 and Theorem 3.19:

Equation 3.82 gives

$$L(\rho, s)^n \prod L(\mathrm{Ind}\, \psi_i, s) = \prod L(\mathrm{Ind}\, \psi'_j, s) \tag{3.83}$$

$$\Rightarrow \qquad L(\rho, s)^n = \frac{\prod L(\mathrm{Ind}\, \psi'_j, s)}{\prod L(\mathrm{Ind}\, \psi_i, s)} \tag{3.84}$$

The numerator and denominator of the fraction are both analytic, thus $L(\rho, s)^n$ meromorphic $\square$

Corollary 3.22
If ρ irreducible non-trivial, then $L(\rho, s)$ is analytic and non-zero at $s = 1$

Proof
Write R for the regular representation of $\mathrm{Gal}(F/K)$. Then

$$\begin{aligned} \zeta_F(s) &= L(F/K,R,s) \qquad \text{Prop 3.18(iii)} && (3.85)\\ &= \prod T \text{ irred.} L(F/K,T,s)^{\dim T} && (3.86)\\ &= \zeta_K(s) \prod_{\text{irred } T\neq \mathbb{1}} L(F/K,T,s)^{\dim T} && (3.87) \end{aligned}$$

$\zeta_F(s), \zeta_K(s)$ have simple poles at $s=1$
$\Rightarrow^*$ $L(\rho,s)^n$ cannot have a zero at $s=1$
$\Rightarrow$ $L(\rho,s)$ can be analytically continued to $s=1$ and is non-zero there.
(*: using $L(T,s)$ are bounded at $s=1$) $\square$

Theorem 3.23 (Artin-Brauer (non-examinable))
$L(\rho,s)$ is meromorphic on all of $\mathbb{C}$

Lemma 3.24
(This lemma strengthen Theorem 3.19) F/K Galois, $\rho \neq \mathbb{1}$ 1-dimensional representation of $\mathrm{Gal}(F/K)$. Then $L(\rho,\mathbb{1}) \neq 0$

Proof
By Proposition 3.18(ii) we may assume that ρ is faithful, so $\mathrm{Gal}(F/K)$ is abelian (cyclic). Then (by Proposition 3.18(i),(iii))

$$\zeta_F(s) = \prod_{\chi \text{1-dim repn of } \mathrm{Gal}(F/K)} L(\chi,s) = \zeta_K(s) \prod_{\chi\neq\mathbb{1}} L(\chi,s) \tag{3.88}$$

As ζ_F, ζ_K have a simple pole at $s=1$ and all other $L(\chi,s)$ are analytic there, it follows that $L(\chi,\mathbb{1}) \neq 0$
In particular, $L(\rho,\mathbb{1}) \neq 0$ $\square$

3.6 Density Theorems

Definition 3.25
Let S be a set of prime numbers. Then S has Dirichlet density α if

$$\sum_{p\in S} \frac{p^{-s}}{\log \frac{1}{1-s}} \to \alpha \quad \text{as} \quad s \to 1^+ \tag{3.89}$$

Example:
By Dirichlet's Theorem (Theorem 3.12)

- The set of all primes has density 1
- $S_{a,N} = \{p \text{ prime}, p \cong a \mod N\}$ has density $\frac{1}{\phi(N)}$ whenever $(a,N)=1$

Notation:
For $F/\mathbb{Q}$ Galois, p unramified in F, write $\mathrm{Frob}_p \in \mathrm{Gal}(F/\mathbb{Q})$ for the Frobenius element $\mathrm{Frob}_{\mathfrak{q}/p}$ of some prime $\mathfrak{q}$ above p. Note that it lies in well-defined conjugacy class of $\mathrm{Gal}(F/\mathbb{Q})$, as (c.f. Example Sheet 2)

$$\mathrm{Frob}_{\mathfrak{q}'/p} = x\,\mathrm{Frob}_p\,x^{-1} \quad \text{when } \mathfrak{q}' = x(\mathfrak{p}) \tag{3.90}$$

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 $p \nmid N$, $\mathrm{Frob}_p = \sigma_a \Leftrightarrow p \cong a \mod N$ (as $\mathrm{Frob}_p(\zeta_N) = \zeta_N^p$)
So Dirichlet Theorem $\Rightarrow$

$$S_{N,\sigma} = \{p \nmid N, \mathrm{Frob}_p = \sigma\} \text{ has Dirichlet density } \frac{1}{|\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})|}$$

i.e. Frob_p is "uniformly distributed" among $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$

Theorem 3.26 (Chebotarev's Density Theorem)
Let $F/\mathbb{Q}$ be a finite Galois extension and $\mathcal{C}$ conjugacy class of $\mathrm{Gal}(F/\mathbb{Q})$. Then

$$S_{\mathcal{C}} = \{p \text{ unramified in } F/\mathbb{Q} \text{ s.t. } \mathrm{Frob}_p \in \mathcal{C}\} \text{ has Dirichlet density } \tfrac{|\mathcal{C}|}{|\mathrm{Gal}(F/\mathbb{Q})|}$$

Corollary 3.27 (Frobenius)
let $f(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial. The set of primes p such that $f(X) \mod p$ factorises as a product of irreducible polynomials of degree $d_1, \dots, d_n$ has Dirichlet density:

$$\frac{|\{g \in \mathrm{Gal}(f) \text{ has cycle type } (d_1, d_2, \dots, d_n) \text{ on roots of } f\}|}{|\mathrm{Gal}(f)|} \tag{3.91}$$

Proof
$f(X) \mod p$ has a repeated root in $\overline{\mathbb{F}_p}$ modulo only finitely many primes.
For the rest, Frob_p acts as an element of cycle type $(d_1, \dots, d_n)$ where these are the degrees of the irreducible factors of $f(X) \mod p$ $\square$

Example:
$f(X)$ irreducible quintic, with Galois group S_5

- prime p s.t. $f(X) \mod p$ is irreducible has density $\frac{|\{5\text{−cycles in } S_5\}|}{120} = \frac{24}{120} = \frac{1}{5}$
- primes p s.t. $f(X) \mod p$ splits into linear factors has density $\frac{1}{120}$
- primes p s.t. $f(X) \mod p =$ quadratic$\times$cubic has density $\frac{20}{120} = \frac{1}{6}$

Corollary 3.28
If $f(X) \in \mathbb{Z}[X]$ monic irreducible with $\deg f > 1$, then $f(X) \mod p$ has no root in $\mathbb{F}_p$ for infinitely many primes p

Proof
Sufficient to prove: $\exists g \in \mathrm{Gal}(F/\mathbb{Q})$ that fixes no root of $f(X)$

But $\bigcup_{\alpha \text{ roots}} \mathrm{Stab}_{\mathrm{Gal}(f)}(\alpha) \neq \mathrm{Gal}(f)$ since each $\mathrm{Stab}(\alpha)$ has size $\frac{|\mathrm{Gal}(f)|}{\deg f}$ and each contains the identity element $\square$

Proof of Chebotarev's Density Theorem 3.26
For ρ irreducible representation of $\mathrm{Gal}(F/\mathbb{Q})$, let

$$L_*(\rho, s) = \prod_{p \text{ unram.}} P_p(\rho, p^{-s})^{-1} \tag{3.92}$$

Step 1:
By Example Sheet 1 Q10, only finitely many primes ramify in $F/\mathbb{Q}$, so Corollary 3.22 $\Rightarrow$:

- $L_*(\rho, s) \neq 0, \infty$ at $s = 1$ if $\rho \neq \mathbb{1}$ irreducible
- $L_*(\mathbb{1}, s)$ has a simple pole at $s = 1$

Step 2:
Write χ_p for the character of ρ. If ρ unramified in $F/\mathbb{Q}$, and $\lambda_1, \ldots, \lambda_d$ are the eigenvectors (with multiplicities) of Frob_p on ρ, then

$$\begin{aligned}
\log \frac{1}{P_p(\rho, p^{-s})} &= \log \frac{1}{\pi(1-\lambda_i p^{-s})} && (3.93)\\
&= \sum_i \log\left(\frac{1}{1-\lambda_i p^{-s}}\right) && (3.94)\\
&= \left(\sum \lambda_i\right) p^{-s} + \left(\frac{\sum \lambda_i^2}{2}\right) p^{-2s} + \left(\frac{\sum \lambda_i^3}{3}\right) p^{-3s} + \cdots && (3.95)\\
&= \sum_{n\geq 1} \frac{\chi_p(\mathrm{Frob}_p^n)}{n} p^{-ns} && (3.96)
\end{aligned}$$

The Dirichlet series

$$\sum_{p \text{ unram.}} \sum_{n\geq 1} \frac{\chi_p(\mathrm{Frob}_p^n) p^{-ns}}{n} \tag{3.97}$$

has bounded coefficients, so (c.f. Proof of Proposition 3.10) defines an analytic branch of $\log L_*(\rho, s)$ on $\mathrm{Re}(s) > 1$. Now

$$\sum_{p \text{ unram.}} \sum_{n\geq 2} \frac{\chi_p(\mathrm{Frob}_p^n) p^{-ns}}{n} \tag{3.98}$$

is bounded on $\mathrm{Re}(s) > 1$ by $2 \dim \rho \displaystyle\sum_{k=1}^{\infty} \frac{1}{k^2}$ (c.f. Proof of Corollary 3.11), so

- $f_p(s) = \displaystyle\sum_{p \text{unram}} \chi_p(\mathrm{Frob}_p) p^{-s}$ is bounded as $s \to 1$ on $\mathrm{Re}(s)$ if $\rho \neq \mathbb{1}$ (by Step 1)
- $f_{\mathbb{1}}(s) = \displaystyle\sum_{p \text{unram}} p^{-s} \sim \log \frac{1}{1-s}$ as $s \to 1$

Step 3:

$$\begin{aligned}
\sum_{p \in S_{\mathcal{C}}} p^{-s} &= \sum_{p \text{ unram}} C_{\mathcal{C}}(\mathrm{Frob}_p) p^{-s} && (3.99)\\
&= \sum_{\rho} \langle \chi_\rho, C_{\mathcal{C}} \rangle f_\rho(s) && (3.100)\\
&= \frac{|\mathcal{C}|}{|\operatorname{Gal}(F/\mathbb{Q})|} f_{\mathbb{1}}(s) + \sum_{\rho \neq \mathbb{1}} \langle \chi_\rho, C_{\mathcal{C}} \rangle f_\rho(s) && (3.101)
\end{aligned}$$

where

$$C_{\mathcal{C}}(g) = \begin{cases} 0 & g \notin \mathcal{C} \\ 1 & g \in \mathcal{C} \end{cases} \tag{3.102}$$

Hence $S_{\mathcal{C}}$ has density $\dfrac{|\mathcal{C}|}{|\operatorname{Gal}(F/\mathbb{Q})|}$ □

(End of examinable material)

Remark. Exam is 2 hours long, to complete 3 questions out of 4 questions, about 50% bookwork.
For representation theory, you should know for $C_2 \times C_2, S_3$, cyclic groups, D_8, D_10 (with hint), D_{2n}, S_4, A_4, Q_8, abelian groups (with help sometimes)
For Galois theory, what you *must* know includes finite fields $\mathbb{F}_q$ and cyclotomic fields $\mathbb{Q}(\zeta_n)$
For complex analysis, nothing beyond bookwork (i.e. this lecture notes) is needed

4 Local Fields

(Warining: This section may be exambinable for Local Fields)

Definition 4.1
A place in a number field K is an equivalence class of (non-trivial) absolute values on K

There are two functors:

- infinte places v (correspond to archimedean absolute values) cam from embedding $K \hookrightarrow \mathbb{R}$ or $K \hookrightarrow \mathbb{C}$ and taking
$$|x|_v = \begin{cases} |x| & \text{for real embeddings} \\ |x|^2 & \text{for complex ones} \end{cases} \tag{4.1}$$
(these are the usual normalisations)
(Note: Complex conjugate embeddings give same $| \ |_v$)
Fact: The rest don't and each archimedean absolute value arises in this way
$\Rightarrow$ number of infinite places of $K = r_1 + r_2$
- finite places (correspond to non-archimedean absolute values) correspond to primes of K:
If $\mathfrak{p}$ is a prime, set $|x|_\mathfrak{p} = N(\mathfrak{p})^{-\mathrm{ord}_\mathfrak{p}(x)}$, where $\mathrm{ord}_\mathfrak{p}(x)$ for $x \in \mathcal{O}_K$ is the power of $\mathfrak{p}$ in factorisation of (x) and extended multiplicatively to $K^\times$
Fact: (Ostrowski) These are inequivalent (for different $\mathfrak{p}$) and there are no others

Completions: $| \ |_v$ makes K into a metric space. Its completion K_v is a complete local field

v archimedean $\Rightarrow$ K_v $\mathbb{R}$ or $\mathbb{C}$ (this is boring to number theorists)
Hence forth assume v is a finite place

If $K = \mathbb{Q}$ and v correspond to p, then $K_v = \mathbb{Q}_p$
If K general, v corresponds to $\mathfrak{q}$ which lies above $p \in \mathbb{Z}$ then $| \ |_v$ restricted to $\mathbb{Q}$ is equivalent to $| \ |_p$
$\Rightarrow$ K_v is a finite extension of $\mathbb{Q}_p$

4.1 Residue field and ramification

K number field, $| \ |_v$ absolute value corresponding to $\mathfrak{q}$
$\mathcal{O}_{K_v} \subseteq K_v$ (elements with $|x|_v \leq 1$)
$\mathcal{O}_{K_v}^\times =$ units (elements with $|x|_v = 1$)
$\mathfrak{m}_v =$ maximal ideal of $\mathcal{O}_{K_v}$ (elements with $|x|_v < 1$)
$k_v = \mathcal{O}_{K_v} / \mathfrak{m}_v =$ residue field

Observe $\mathfrak{q} \subset \mathfrak{m}_v$, $\mathcal{O}_K \subseteq \mathcal{O}_{K_v}$, $\mathcal{O}_K / \mathfrak{q} \to k_v$

- is injective (clear: a field homomorphism)
- surjective (every element of K_v can be approximated by an element of K)

$$\Rightarrow \quad \mathcal{O}_K / \mathfrak{q} = k_v \text{ - residue field does not change by completion}$$

If L/K field extension, $\mathfrak{r}$ lies above $\mathfrak{q}$ (and $| \ |_w$ correspond to $\mathfrak{r}$)

$$\Rightarrow \quad L_w/K_v \quad \text{finite} \tag{4.2}$$
$$f_{\mathfrak{r}/\mathfrak{q}} = f_{w/v} \quad \text{(by bove)} \tag{4.3}$$
$$e_{\mathfrak{r}/\mathfrak{q}} = e_{w/v} \quad \text{(compare valuations)} \tag{4.4}$$

4.2 Galois Groups

F/K Galois extension of number fields, $\mathfrak{q}$ lies above $\mathfrak{p}$, $|\ |_w, |\ |_v$ corresponding absolute values respectively.

If $g \in D_{\mathfrak{q}\,/\,\mathfrak{p}}$ then it preserve $|\ |_w$

$\Rightarrow$ it is a topoogical equivalence

$\Rightarrow$ it extends to an automorphism of F_w

$\Rightarrow$ we get $D_{\mathfrak{q}\,/\,\mathfrak{p}} \to \mathrm{Gal}(F_w/K_v)$

Lemma 4.2
This is an isomorphism

Sketch Proof
Injective: easy
Surjective: $\left|D_{\mathfrak{q}\,/\,\mathfrak{p}}\right| = e_{\mathfrak{q}\,/\,\mathfrak{p}} f_{\mathfrak{q}\,/\,\mathfrak{p}} = e_{w/v} f_{w/v} = [F_w : K_v] = |\mathrm{Gal}(F_w/K_v)|$ □

Observe also that $I_{\mathfrak{q}\,/\,\mathfrak{p}} \xrightarrow{\sim} I_{w/v}$ also isomorphic
(being the element that act trivially on respective residue field)

4.3 Applications

Proposition 4.3
If $f(X) \in \mathcal{O}_K[X]$ is Eisenstien w.r.t $\mathfrak{p}$ and α a root
then $K(\alpha)/K$ has degree $= \deg f$ and is totally ramified at $\mathfrak{p}$

Proof
Complete and invert Local Fields course □

Proposition 4.4
Decomposition groups are soluble

Proof
Galois groups of finite extensions of $\mathbb{Q}_p$ are soluble:
$I \trianglelefteq G, G/I$ cyclic
$I_1 \trianglelefteq I$ with I_1/I cyclic (I_1 =wild inertia group)
I_1 is a p-group □

Example 4.5
There are no C_4-extensions at $\mathbb{Q}$ where quadratic subfield is $\mathbb{Q}(\zeta_3)$

Proof
$\mathbb{Q}(\zeta_3)/\,\mathbb{Q}$ ramified at 3
$\Rightarrow$ Inertia at 3 must be all of C_4

Complete at (the prime of F above) 3, get $F_w/\,\mathbb{Q}_3$ toatally ramified, cyclic of degree 4.

But this is a tame extension (since $3 \nmid 4$) $\Rightarrow$ $\mathrm{Gal}(F_w/\,\mathbb{Q}_3) \hookrightarrow \mathbb{F}_3^\times$
which is nonsense # □