A second course in Algebraic Number Theory

Vlad Dockchitser

Prerequisites:

- Galois Theory
- Representation Theory

Overview:

1. Number Fields (Review, $K, \mathcal{O}_K, \mathcal{O}^*, \mathrm{Cl}_K$, etc)
2. Decomposition of primes (how primes behave in field extensions and what does Galois's do)
3. L-series (Dirichlet's Theorem on primes in arithmetic progression, Artin L-functions, Cheboterev's density theorem)

1 Number Fields

1.1 Rings of integers

Definition 1.1. A *number field* is a finite extension of $\mathbb{Q}$

Definition 1.2. An *algebraic integer α is an algebraic number that satisfies a monic polynomial with integer coefficients*

Definition 1.3. Let K be a number field. It's *ring of integer* $\mathcal{O}_K$ consists of the elements of K which are algebraic integers

Proposition 1.4.

1. *$\mathcal{O}_K$ is a (Noetherian) Ring*
2. $\mathrm{rk}_{\mathbb{Z}}\, \mathcal{O}_K = [K : \mathbb{Q}]$*, i.e.,* $\mathcal{O}_K \cong \mathbb{Z}^{[K:\mathbb{Q}]}$ *as an abelian group*
3. *Each $\alpha \in K$ can be written as $\alpha = \beta/n$ with $\beta \in \mathcal{O}_K$ and $n \in \mathbb{Z}$*

Example.

K	$\mathcal{O}_K$
$\mathbb{Q}$	$\mathbb{Z}$
$\mathbb{Q}(\sqrt{a})$ ($a \in \mathbb{Z} \setminus \{0,1\}$,$a$ square free)	$\begin{cases} \mathbb{Z}[\sqrt{a}] & a \equiv 2,3 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{a}}{2}] & a \equiv 1 \mod 4 \end{cases}$
$\mathbb{Q}(\zeta_n)$ where ζ_n is a primitive nth root of unity	$\mathbb{Z}[\zeta_n]$

Proposition 1.5.

1. *$\mathcal{O}_K$ is the maximal subring of K which is finitely generated as an abelian group*
2. *$\mathcal{O}`_K$ is integrally closed - if $f \in \mathcal{O}_K[x]$ is monic and $f(\alpha) = 0$ for some $\alpha \in K$, then $\alpha \in \mathcal{O}_K$.*

Example (Of Factorisation)**.** $\mathbb{Z}$ is UFD. When factorisation can only get different orders of factors and different signs. The latter come from the units ± 1 in $\mathbb{Z}$.

$\mathcal{O}_K$ may not even be a UFD, e.g., $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

To fix this one works with ideals.

1.2 Units

Definition 1.6. A *unit* in a number field K is an element α of $\mathcal{O}_K$ with $\alpha^{-1} \in \mathcal{O}_K$. The group of units is denoted $\mathcal{O}_K^*$.

Example.

K	$\mathcal{O}_K$	$\mathcal{O}_K^*$
$\mathbb{Q}$	$\mathbb{Z}$	$\{\pm 1\}$
$\mathbb{Q}(i)$	$\mathbb{Z}[i]$	$\{\pm 1, \pm i\}$
$\mathbb{Q}\left(\sqrt{2}\right)$	$\mathbb{Z}[\sqrt{2}]$	$\left\{\pm(1+\sqrt{2})^n : n \in \mathbb{Z}\right\}$

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

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

where Δ is the (finite) group of roots of unity in K, r_1 is the number of distinct embeddings of K into $\mathbb{R}$, r_2 the number of pairs of complex conjugates K into $\mathbb{C}$ with image not in $\mathbb{R}$. (Hence $r_1 + 2r_2 = [K : \mathbb{Q}]$)

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

1.3 Ideals

Example. $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$, $\underline{a} = (17)$ =all multiples of 17. So $\alpha \in \underline{a}$ if and only if $\alpha = 17n$ for some $n \in \mathbb{Z}$. Multiplication: $(3) \cdot (17) = (51)$.

Unique factorisation of ideals. *Let Kbe a number field. Every non-zero ideals of $\mathcal{O}_K$ admits a factorisation into prime ideals. This factorisation is unique up to order.*

Definition 1.7. Let $\underline{a}, \underline{b} \lhd \mathcal{O}_K$ be two ideals. Then $\underline{a}$ *divides* $\underline{b}$ (written $\underline{a}|\underline{b}$) if $\underline{a} \cdot c = \underline{b}$ for some ideal $\underline{c}$. (Equivalently if in the prime factorisation, $\underline{a} = p_1^{n_1} \cdots p_k^{n_k}, \underline{b} = p_1^{m_1} \dots p_k^{m_k}$ we have $n_i \leq m_i$ for all i)

Remark.

1. For $\alpha, \beta \in \mathcal{O}_K$, $(\alpha) = (\beta)$ if and only if $\alpha = \beta u$ for some $u \in \mathcal{O}_K^*$.
2. For ideals $\underline{a}, \underline{b}$ then $\underline{a}|\underline{b}$ if and only $\underline{a} \supseteq \underline{b}$.
3. To multiply ideals, just multiply their generators, e.g. $(2) \cdot (3) = (6)$, $(2, 1+\sqrt{-5}) \cdot (2, 1-\sqrt{-5}) = (4, 2+2\sqrt{-5}, 2-2\sqrt{-5}, 6) = (2)$
4. To add ideals, combine their generators, e.g., $(2) + (3) = (2, 3) = (1) = \mathcal{O}_K$.

Lemma 1.8. *$\underline{a}, \underline{b} \lhd \mathcal{O}_K$, $\underline{a} = \prod_i p_i^{n_i}$, $\underline{b} = \prod_i p_i^{m_i}$ with $n_i, m_i \geq 0$ and p_i prime ideals. Then*

1. $\underline{a} \cap \underline{b} = \prod_i p_i^{\max(n_i, m_i)}$ *(lowest common multiple)*
2. $\underline{a} + \underline{b} = \prod_i p_i^{\min(n_i, m_i)}$ *(greatest common divisor)*

Lemma 1.9. *Let $\alpha \in \mathcal{O}_K \setminus \{0\}$. Then there exists $\beta \in \mathcal{O}_K \setminus \{0\}$ such that $\alpha\beta \in \mathbb{Z} \setminus \{0\}$.*

Proof. Let $X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ (with $a_i \in \mathbb{Z}$) be the minimal polynomial of α. Then $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + \alpha_1\alpha = -a_0 \in \mathbb{Z}$, so take $\beta = \alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1$. □

Corollary 1.10. *If $\underline{a} \lhd \mathcal{O}_K$ is a non-zero ideal, then $[\mathcal{O}_K : \underline{a}]$ is finite.*

Proof. Pick $\alpha \in \underline{a} \setminus \{0\}$ and $\beta \in \mathcal{O}_K$ with $N = \alpha\beta \in \mathbb{Z} \setminus \{0\}$. Then $N \in \underline{a}$ and $[\mathcal{O}_K : \underline{a}] \leq [\mathcal{O}_K : (\alpha)] \leq [\mathcal{O}_K : (N)] = [\mathcal{O}_K : N\mathcal{O}_K] = |N|^{[K:\mathbb{Q}]}$ (By Proposition 1.4) □

Definition 1.11. The *norm* of a non-zero ideal $\underline{a} \lhd \mathcal{O}_K$ is $N(\underline{a}) = [\mathcal{O}_K : \underline{a}]$.

Lemma 1.12. *Let $\alpha \in \mathcal{O}_K \setminus \{0\}$, then $\left|N_{K/\mathbb{Q}}(\alpha)\right| = N((\alpha))$*

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

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

□

1.4 Ideal Class Group

Let K be a number field. We can define an equivalence relation on non-zero ideals of $\mathcal{O}_K$ by $\underline{a} \sim \underline{b}$ if and only if there exists $\lambda \in K^*$ such that $\underline{a} = \lambda \underline{b}$. The *ideal class group* of K denoted Cl_K, is the set of classes $\{$non-zero ideals$\}/\sim$. It is a group, the group structure coming from multiplication of ideals. The identity is $\{$principal ideals$\}$ and $\mathcal{O}_K$. Note that PID if and only if $\mathrm{Cl}_K = 1$ if and only if UFD

Theorem 1.13. Cl_K *is finite*

1.5 Primes and Modular Arithmetic

Definition 1.14. A *prime* $\underline{p}$ in a number field K is a non-zero prime ideal in $\mathcal{O}_K$

Its *residue field* is $\mathcal{O}_K/\underline{p} = \mathbb{F}_{\underline{p}}$.

Its *residue characteristic,* p, is the characteristic of $\mathcal{O}_K/\underline{p}$.

Its (absolute) *residue degree* is $f_{\underline{p}} = \left[\mathcal{O}_K/\underline{p} : \mathbb{F}_p\right]$.

Lemma 1.15. *The residue field of a prime is indeed a finite field.*

Proof. Let $\underline{p}$ be a prime, then $\mathcal{O}_K/\underline{p}$ is an integral domain. Furthermore $\left|\mathcal{O}_K/\underline{p}\right| = \left[\mathcal{O}_K : \underline{p}\right] = N(\underline{p})$ which is finite by Corollary 1.10. Hence $\mathcal{O}_K/\underline{p}$ is a field. □

Note. The size of the residue field is $N(\underline{p})$

Example. Let $K = \mathbb{Q}$ then $O_K = \mathbb{Z}$. Let $\underline{p} = (17)$, then the residue field $\mathcal{O}_K/\underline{p} = \mathbb{Z}/(17) = \mathbb{F}_{17}$.

Let $K = \mathbb{Q}(i)$ then $\mathcal{O}_K = \mathbb{Z}[i]$. Let $\underline{p} = (2+i)$, then $\mathcal{O}_K/\underline{p} = \mathbb{F}_5$ and its representatives can be $\{0, 1, 1+i, 2i, 2i+1\}$. Let $\underline{p} = (3)$, then $\mathcal{O}_K/\underline{p} = \mathbb{F}_9$ (= "$\mathbb{F}_3[i]$")

Let $K = \mathbb{Q}(\sqrt{d})$ where $d \equiv 2, 3 \mod 4$, so $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{d}\right]$. Let $\underline{p}$ be a prime with residue characteristic p, then $\mathcal{O}_K/\underline{p}$ is generated by $\mathbb{F}_p$ and the image of $\sqrt{d}$. Thus $\mathcal{O}_K/\underline{p} = \mathbb{F}_p\left[\sqrt{d}\right] = \begin{cases} \mathbb{F}_p & \text{if } d \text{ a square mod } p \\ \mathbb{F}_{p^2} & \text{else} \end{cases}$

Notation. If $\underline{a} \lhd \mathcal{O}_K$ is a non-zero ideal, we say that $x \equiv y \mod \underline{a}$ if $x - y \in \underline{a}$.

Theorem 1.16 (Chinese Remainder Theorem)**.** *Let K be a number field and $\underline{p}_1, \dots, \underline{p}_k$ be distinct primes. Then*

$$\mathcal{O}_K/\left(\underline{p}_1^{n_1} \dots \underline{p}_k^{n_k}\right) \to \mathcal{O}_K/\underline{p}_1^{n_1} \times \dots \times \mathcal{O}_K/\underline{p}_k^{n_k}$$

via $x \mod \underline{p}_1^{n_1} \dots \underline{p}_k^{n_k} \mapsto \left(x \mod \underline{p}_1^{n_1}, \dots, x \mod \underline{p}_k^{n_k}\right)$ is a ring isomorphism.

Proof. Let $\psi : \mathcal{O}_K \to \mathcal{O}_K/\underline{p}_1^{n_1} \times \dots \times \mathcal{O}_K/\underline{p}_k^{n_k}$ by $x \mapsto \left(x \mod \underline{p}_1^{n_1}, \dots, x \mod \underline{p}_k^{n_k}\right)$. This is a ring homomorphism with $\ker \psi = \cap_{i=1}^k \underline{p}_i^{n_i} = \prod_{i=1}^k \underline{p}_i^{n_i}$ (by Lemma 1.8).

So it remains to prove that ψ is surjective, so that we can apply the first isomorphism theorem. By Lemma 1.8, $\underline{p}_j^{n_j} + \prod_{i \neq j} \underline{p}_i^{n_i} = \mathcal{O}_K$, so there $\alpha \in \underline{p}_j^{n_j}$ and $\beta \in \prod_{i \neq j} \underline{p}_i^{n_i}$ such that $\alpha + \beta = 1$, now $\beta \equiv 0 \mod \underline{p}_i^{n_i}$ for all $i \neq j$ and $\beta \equiv 1 \mod \underline{p}_j^{n_j}$. So $\mathrm{im}\, \psi \ni \psi(\beta) = (0, 0, \dots, 0, 1, 0, \dots, 0)$. This is true for all j, hence ψ is surjective. □

Remark. CRT implies that we can solve any system of congruences, i.e., $x \equiv a_i \mod \underline{p}_i^{n_i}$ for $1 \leq i \leq k$. (This is called the Weak Approximation Theorem)

Lemma 1.17. *Let $\underline{p} \lhd \mathcal{O}_K$ be prime*

1. $\left|\mathcal{O}_K/\underline{p}^n\right| = N(\underline{p})^n$
2. $\underline{p}^n/\underline{p}^{n+1} = \mathcal{O}_K/\underline{p}$ *as $\mathcal{O}_K$-module*

Proof. 2. implies 1. as

$$\begin{aligned} \left|\mathcal{O}_K/\underline{p}^n\right| &= \left|\mathcal{O}_K/\underline{p}\right| \cdot \left|\underline{p}/\underline{p}^2\right| \cdots \left|\underline{p}^n/\underline{p}^{n+1}\right| \\ &= N(\underline{p})^n \end{aligned}$$

2.) By unique factorisation $\underline{p}^n \neq \underline{p}^{n+1}$, so pick $\pi \in \underline{p}^n \setminus \underline{p}^{n+1}$. Thus $\underline{p}^n | (\pi)$ and $\underline{p}^{n+1} \nmid (\pi)$. So $(\pi) = \underline{p}^n \cdot \underline{a}$ with $\underline{p} \nmid \underline{a}$. So define $\phi : \mathcal{O}_K \to \mathcal{O}_K/\underline{p}^{n+1}$ by $\phi(x) = \pi x \mod \underline{p}^{n+1}$, an $\mathcal{O}_K$-map. Note that $\ker \phi = \left\{x : \underline{p}^{n+1} | (\pi x)\right\} = \underline{p}$ and $\operatorname{im} \phi = (\pi) + \underline{p}^{n+1} \mod \underline{p}^{n+1} = \underline{p}^n \mod \underline{p}^{n+1}$ (by Lemma 1.8). Hence $\mathcal{O}_K/\underline{p} \xrightarrow{\cong} \underline{p}^n/\underline{p}^{n+1}$. □

Corollary 1.18. $N(\underline{ab}) = N(\underline{a})N(\underline{b})$.

Proof. Use Theorem 1.16 and Lemma 1.17. □

Lemma 1.19. $N(\underline{a}) \in \underline{a}$

Proof. $N(\underline{a})$ is zero in any abelian group of order $N(\underline{a})$, in particular in $\mathcal{O}_K/\underline{a}$. □

1.6 Enlarging the field

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

- $(2) = (1+i)^2$
- (3) remains prime
- $(5) = (2+i)(2-i)$

We only see those three properties/behaviour in $\mathbb{Q}(i)$, so we say

- "2 ramifies"
- "3 is inert"
- "5 splits"

Note that $\underline{p}$ (prime of $\mathbb{Q}(i)$) contains $p = \operatorname{char}\mathbb{Z}[i]/\underline{p}$, so $\underline{p}|(p)$. Thus factorising $2, 3, 5, 7, \ldots$ will yield all the primes of $\mathbb{Z}[i]$.

Definition 1.20. Let L/K be an extension of number fields and $\underline{a} \lhd \mathcal{O}_K$ an ideal. Then the *conorm* of $\underline{a}$ is the ideal $\underline{a}\mathcal{O}_L$ of $\mathcal{O}_L$. I.e., the ideal generated by the elements of $\underline{a}$ in $\mathcal{O}_L$. Equivalently, if $\underline{a} = (\alpha_1, \ldots, \alpha_n)$ as an $\mathcal{O}_K$-ideal, then $\underline{a}\mathcal{O}_L = (\alpha_1, \ldots, \alpha_n)$ as an $\mathcal{O}_L$-ideal.

Note. $(\underline{a}\mathcal{O}_L)(\underline{b}\mathcal{O}_L) = (\underline{ab})\mathcal{O}_L$
$(\underline{a}\mathcal{O}_M) = (\underline{a}\mathcal{O}_L)\mathcal{O}_M$ when $K \leq L \leq M$
Warning: Sometimes write $\underline{a}$ for $\underline{a}\mathcal{O}_L$.

Proposition 1.21. *Let L/K be an extension of number fields and $\underline{a} \in \mathcal{O}_K$ a non-zero ideal. Then $N(\underline{a}\mathcal{O}_L) = N(\underline{a})^{[L:K]}$.*

Proof. If $\underline{a} = (\alpha)$ is principal, then by Lemma 1.12, we get

$$\begin{aligned} N(\underline{a}\mathcal{O}_L) &= \left|N_{L/\mathbb{Q}}(\alpha)\right| \\ &= \left|N_{K/\mathbb{Q}}(\alpha)\right|^{[L:K]} \\ &= |N(\underline{a})|^{[L:K]} \end{aligned}$$

In general, as Cl_K is finite, $\underline{a}^k = (\alpha)$ for some $k \geq 1$. Hence

$$\begin{aligned} N(\underline{a}\mathcal{O}_L)^k &= N(\underline{a}^k\mathcal{O}_L) \\ &= N(\underline{a}^k)^{[L:K]} \\ &= N(\underline{a})^{k[L:K]} \end{aligned}$$

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

Definition 1.22. A prime $\underline{q}$ of L *lies above* a prime of K if $\underline{q}|\underline{p}\mathcal{O}_L$. (Equivalently if $\underline{q} \supseteq \underline{p}$ as sets)

Lemma 1.23. *Let L/K be a number field. Every prime of L lies above a unique prime of K. In fact $\underline{q}$ lies above $\underline{q} \cap \mathcal{O}_K = \underline{p}$.*

Proof. $\underline{q} \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ and is non-zero as it contains $N(\underline{q})$. So $\underline{q}$ lies above $\underline{p} = \underline{q} \cap \mathcal{O}_K$.

If $\underline{q}$ also lies above $\underline{p}'$ then $\underline{q} \supseteq \underline{p} + \underline{p}' = \mathcal{O}_K \ni \{1\}$, which is a contradiction. □

Lemma 1.24. *Suppose $\underline{q} \lhd \mathcal{O}_L$ lies above $\underline{p} \lhd \mathcal{O}_K$ (primes). Then $\mathcal{O}_L/\underline{q}$ is a field extension of $\mathcal{O}_K/\underline{p}$ with $\phi : \mathcal{O}_K/\underline{p} \hookrightarrow \mathcal{O}_L/\underline{q}$ given by $\phi(x \mod \underline{p}) = x \mod \underline{q}$.*

Proof. ϕ is well-define as $\underline{q} \supseteq \underline{p}$ and is a ring homomorphism, so has no kernel as $\mathcal{O}_K/\underline{p}$ is a field. Hence ϕ is an embedding $\mathcal{O}_K/\underline{p} \hookrightarrow \mathcal{O}_L/\underline{q}$ □

Definition 1.25. If $\underline{q}$ lies above $\underline{p}$ then its *residue degree* is $f_{\underline{q}/\underline{p}} = [\mathcal{O}_L/\underline{q} : \mathcal{O}_K/\underline{p}]$.

Its *ramification degree* is the exponent, $e_{\underline{q}/\underline{p}}$, in the prime factorisations $\underline{p}\mathcal{O}_L = \prod_{i=1}^{n} \underline{q}_i^{e_{\underline{q}_i/\underline{p}}}$.

Theorem 1.26. *Let L/K be an extension of number fields, $\underline{p}$ a prime of K.*

1. *If $\underline{p}\mathcal{O}_L$ decomposes as $\underline{p}\mathcal{O}_L = \prod_{i=1}^{m} \underline{q}_i^{e_i}$ (with $\underline{q}_i$ distinct and $e_i = e_{\underline{q}_i/\underline{p}}$). Then $\sum_{i=1}^{m} e_{\underline{q}_i/\underline{p}} f_{\underline{q}_i/\underline{p}} = [L : K]$.*
2. *If M/L is a further extension, $\underline{r}$ lies above $\underline{q}$, which lies above $\underline{p}$, then $e_{\underline{r}/\underline{p}} = e_{\underline{r}/\underline{q}} e_{\underline{q}/\underline{p}}$ and $f_{\underline{r}/\underline{p}} = f_{\underline{r}/\underline{q}} f_{\underline{q}/\underline{p}}$.*

Proof.

1.

$$\begin{aligned} N(\underline{p})^{[L:K]} &= N(\underline{p}\mathcal{O}_L) \\ &= N(\prod_i \underline{q}_i^{e_i}) \\ &= \prod_i N(\underline{q}_i)^{e_i} \\ &= \prod_i N(\underline{p})^{f_i e_i} \\ &= N(\underline{p})^{\sum e_i f_i} \end{aligned}$$

2. Multiplicativity for e is trivial.

   For f just apply the Tower law

□

Definition 1.27. Let L/K be extensions of number fields, $\underline{p}$ a prime of K with $\underline{p}\mathcal{O}_L = \prod_{i=1}^m \underline{q}_i^{e_i}$ ($\underline{q}_i$ distinct). Then:

- $\underline{p}$ *splits completely* in L if $m = [L:K]$, i.e., $e_i = f_i = 1$
- $\underline{p}$ *splits* in L if $m > 1$
- $\underline{p}$ is *totally ramified* if $m = f = 1$, $e = [L:K]$

We'll see that when L/K is Galois, then $e_j = e_i$ and $f_i = f_j$ for all i, j. Then we say $\underline{p}$ is *ramified* if $e_1 > 1$ and *unramified* if $e_1 = 1$.

Pseudo-example
Let $F = \mathbb{Q}(i)/\mathbb{Q}$, $\mathcal{O}_F = \mathbb{Z}[i]$, and $f(X) = X^2 + 1$
Observe:

$(2) = (i+1)^2 \;\; X^2 + 1 = (X+1)^2 \mod 2$

$(5) = (i+2)(i-2) \;\; X^2 + 1 = (X+2)(X-2) \mod 5$

(3) prime $\;X^2 + 1 \mod 3$ is irreducible

Theorem 1.28 (Kummer - Dedekind)**.** *Let L/K be an extension of number fields. Suppose $\mathcal{O}_K[\alpha] \leq \mathcal{O}_L$ has finite index N , for some $\alpha \in \mathcal{O}_L$ with minimal polynomial $f(X) \in \mathcal{O}_K[X]$. Let $\underline{p}$ be a prime of K not dividing N (equivalently $\mathrm{char}\mathcal{O}_K/\underline{p} \nmid N$).*
If

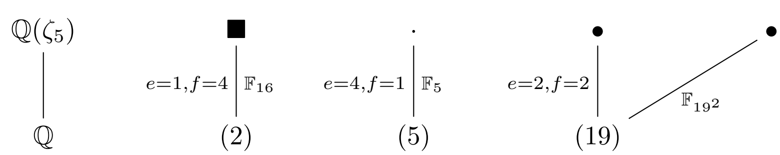
$$f(X) \mod \underline{p} = \prod_{i=1}^m \overline{g}_i(X)^{e_i}$$

where $\underline{g}_i$ are distinct irreducible, then

$$\underline{p}\mathcal{O}_L = \prod_{i=1}^m \underline{q}_i^{e_i}$$

with $\underline{q}_i = \underline{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L$, where $\underline{g}_i(\alpha) \in \mathcal{O}_K[\alpha]$ satisfy $\overline{g}_i(x) = g_i(x) \mod \underline{p}$. The $\underline{q}_i$ are distinct primes of L with $e_{\underline{q}_i/\underline{p}} = e_i$ and $f_{\underline{q}_i/\underline{p}} = \deg \overline{g}_i(X)$.

Example. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_5)$, $\mathcal{O}_L = \mathbb{Z}[\zeta_5]$. Take $\alpha = \zeta_5$, so $N = 1$ and $f(X) = X^4 + X^3 + X^2 + X + 1$.
Now $f(X) \mod 2$ is irreducible, hence (2) is prime in $\mathcal{O}_L$.
$f(X) = (X-1)^4 \mod 5$, hence $(5) = (5, \zeta_5 - 1)^5$
$f(X) = (X^2 + 5X + 1)(X^2 - 4X + 1) \mod 19$, hence $(19) = (19, \zeta_5^2 + 5\zeta_5 + 1)(19, \zeta_5^2 - 4\zeta_5 + 1)$.



Proof of Theorem 1.28.

Claim. 1: $\underline{q}_i$ are primes with $f_{\underline{q}_i/\underline{p}} = \deg \overline{q}_i$
Set $A = \mathcal{O}_K[\alpha]$, $\mathbb{F} = \mathcal{O}_K/\underline{p}$, $p = \mathrm{char}\mathbb{F}$. Use the map $x \mapsto \alpha$ to define a map

$$\begin{aligned} A/\underline{p}A + g_i(\alpha)A \;\; &\leftarrow \;\; \mathcal{O}_K[x]/(f(x), \underline{p}, \underline{g}_i(x)) \\ &\cong \;\; \mathbb{F}[x]/(\overline{f}(x), \overline{g}_i(x)) \\ &\cong \;\; \mathbb{F}[x]/(\overline{g}_i(x)) \end{aligned}$$

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

Now pick $M \in \mathbb{Z}$ such that $NM \equiv 1 \mod p$ and consider $\phi : A/\underline{p}A + g_i(\alpha)A \to \mathcal{O}_L/\underline{q}_i$ defined by $\phi(x) \mod (\underline{p}A + g_i(\alpha)A) \to x \mod \underline{q}_i$, it is well defined as $\underline{q}_i \supseteq \underline{p}A + g_i(\alpha)A$. It is surjective since: if $x \in \mathcal{O}_L$ then $Nx \in A$ and $M(Nx) = MNx \mod \underline{q}_i = x \mod \underline{q}_i$ (since $MN \equiv 1 \mod \underline{q}_i$). Now $\mathcal{O}_L/\underline{q}_i$ is non-zero: otherwise $1 \in \underline{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L$, so both $\underline{p}$ and $MN \in \underline{p}A + g_i(\alpha)A$, hence $1 \in \underline{p}A + g_i(\alpha)A$ a contradiction as this is a proper ideal of A. Therefore $\mathcal{O}_L/\underline{q}_i$ is a field (hence $\underline{q}_i$ is prime) with degree f_i over $\mathbb{F}$.

Claim. 2: $\underline{q}_i \neq \underline{q}_j$ for $i \neq j$

As $\gcd(\overline{g}_i(x), \overline{g}_j(x)) = 1$ can find $\lambda(x), \mu(x) \in \mathcal{O}_K[x]$ such that $\lambda(x)g_i(x) + \mu(x)g_j(x) = 1 \mod \underline{p}$. Then $\underline{q}_i + \underline{q}_j$ contains both $\underline{p}$ and $\lambda(\alpha)g_i(\alpha) + \mu(\alpha)g_j(\alpha) = 1 \mod \underline{p}$, hence $\underline{q}_i + \underline{q}_j = \mathcal{O}_L$

Claim. $\underline{p}\mathcal{O}_L = \prod_i \underline{q}_i^{e_i}$

$$\begin{aligned} \prod_i \underline{q}_i^{e_i} &= \prod_i (\underline{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L) \\ &\subseteq \underline{p}\mathcal{O}_L + \prod g_i(\alpha)^{e_i}\mathcal{O}_L \\ &= \underline{p}\mathcal{O}_L \end{aligned}$$

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

$$\begin{aligned} N(\prod_{i=1}^{m} \underline{q}_i^{e_i}) &= \prod_i |\mathbb{F}|^{e_i f_i} \\ &= |\mathbb{F}|^{\deg f(x)} \\ &= |\mathbb{F}|^{[L:K]} \\ &= N(\underline{p}\mathcal{O}_L) \end{aligned}$$

□

Example. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_{p^n})$, p prime, $\mathcal{O}_L = \mathbb{Z}[\zeta_{p^n}]$ and $\alpha = \zeta_{p^n}$. Then $N = 1$, $f(X) = \frac{X^{p^n}-1}{X^{p^{n-1}}-1}$. Now $f(X) = (X-1)^{p^n - p^{n-1}} \mod p$, hence (p) is totally ramified in $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$.

If $q \neq p$ is also prime, then, working $\mod q$, $\gcd(X^{p^n} - 1, \frac{d}{dx}(X^{p^n} - 1)) = 1$, hence $X^{p^n} - 1$ has no repeated roots in $\overline{\mathbb{F}}_q$. In particular, $f(X) \mod q$ has no repeated factors, so all e_i are 1, i.e., q is unramified in $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$.

Remark. Can't always find α such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. But by Primitive Element Theorem, there exists α such that $[\mathcal{O}_L : \mathcal{O}_K[\alpha]] < \infty$, so can decompose almost all primes.

Proposition 1.29. *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 $f(X) \mod p$ has distinct roots in $\overline{\mathbb{F}}_p$ (equivalently $p \nmid \operatorname{disc} f$) then $[\mathcal{O}_L : \mathbb{Z}[\alpha])$ is coprime to p (so Kummer - Dedekind applies)*

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

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

for some $M \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$ with $|\det M| = [\mathcal{O}_L : \mathbb{Z}[\alpha]]$.

Let F be a splitting field for $f(X)$. Write $\sigma_1, \dots \sigma_n$ for the embeddings of $L \hookrightarrow F$ and $\alpha_i = \sigma(\alpha)$ for the roots of $f(x)$. Then

$$\begin{aligned}
p \nmid \operatorname{disc}(f) &= \prod_{i<j} (\alpha_i - \alpha_j)^2 \\
&= \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^{n-1} & & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-2} \end{vmatrix}^2 \\
&= \det\left(M \begin{pmatrix} \sigma_1(\beta_1) & \cdots & \sigma_n(\beta_1) \\ \vdots & & \vdots \\ \sigma_1(\beta_n) & \cdots & \sigma_n(\beta_n) \end{pmatrix} \right)^2 \\
&= [\mathcal{O}_L : \mathbb{Z}[\alpha]] \cdot B
\end{aligned}$$

for some $B \in \mathcal{O}_F \setminus \{0\}$, hence $p \nmid [\mathcal{O}_L : \mathbb{Z}[\alpha]]$. $\square$

Proposition 1.30. *Let L/K be a finite extension of number fields, $\underline{p}$ a prime of K. Suppose $L = K(\alpha)$ for some $\alpha \in \mathcal{O}_L$ satisfying an Eisenstein minimal polynomial with respect to $\underline{p}$, i.e.,*

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

with $\underline{p}|(a_i)$ and $\underline{p}^2 \nmid (a_0)$. Then $\underline{p}$ is totally ramified in L/K

Proof. Omitted $\square$

2 Decomposition of primes

2.1 Action of the Galois group

Let F/K be a Galois extension of number fields:

- $\operatorname{Gal}(F/K) = \operatorname{Aut}(F/K)$.
- F/K is normal (is $f(X) \in K[X]$ is irreducible and acquire a root in F then f splits completely)
- $|\operatorname{Gal}(F/K)| = [F : K]$
- $H < \operatorname{Gal}(F/K) \to F^H$, $\operatorname{Gal}(F/L) \leftarrow K \leq L \leq F$ a 1-1 correspondence

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

Lemma 2.1. *Let $g \in \operatorname{Gal}(F/K)$:*

1. *$\alpha \in \mathcal{O}_L$ then $g\alpha \in \mathcal{O}_F$*

2. $\underline{a} \in \mathcal{O}_F$ *is an ideal, then* $g(\underline{a}) \lhd \mathcal{O}_F$ *ideal*

3. *Let* $\underline{a}, \underline{b} \lhd \mathcal{O}_F$ *be ideals, then* $g(\underline{a} \cdot \underline{b}) = g(\underline{a})g(\underline{b})$, $g(\underline{a} + \underline{b}) = g(\underline{a}) + g(\underline{b})$.
   If $\underline{q}$ *is a prime of* F *above* $\underline{p}$*, a prime of* K*, then*

4. $g(\underline{q})$ *is a prime of* F *above* $\underline{p}$ *(so* $\mathrm{Gal}(F/K)$ *permutes the primes above* $\underline{p}$*)*

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

Proof. Clear □

Example. Let $K = \mathbb{Q}$, $F = \mathbb{Q}(i)$, then $\mathcal{O}_F = \mathbb{Z}[i]$ and $\mathrm{Gal}(F/K) = C_2 = \{\mathrm{id}, \text{complex conjugation}\}$.
Consider $(1+i)$, it is fixed by $\mathrm{Gal}(F/K)$. (3) is also fixed by $\mathrm{Gal}(F/K)$. But $(2+i)$ and $(2-i)$ are swapped by $\mathrm{Gal}(F/K)$.

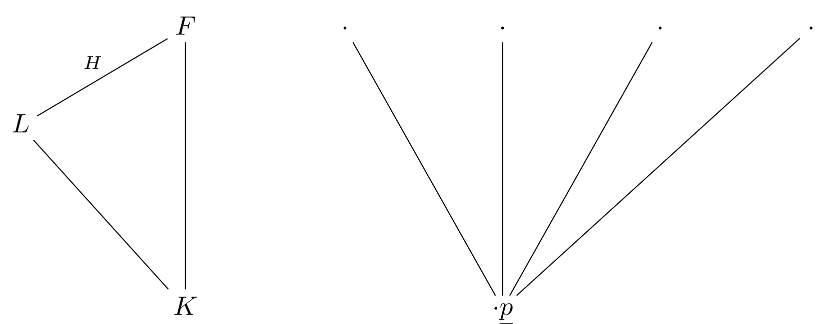
Theorem 2.2. *Let* F/K *be a Galois extension of number fields, let* $\underline{p}$ *be a prime of* K*. Then* $\mathrm{Gal}(F/K)$ *act* <u>*transitively*</u> *on the primes of* F *above* $\underline{p}$*.*

Proof. Let $\underline{q}_1, \dots, \underline{q}_n$ be the primes above $\underline{p}$. We need to show that there exists $g \in \mathrm{Gal}(F/K)$ such that $g(\underline{q}_1) = \underline{q}_2$.
Pick $x \in \mathcal{O}_F$ such that $x \equiv 0 \mod q_1$ but $x \not\equiv 0 \mod q_i$ for all $i \neq 1$. This is possible by the Chinese Remainder Theorem (Theorem 1.16). Then $\prod_{h \in \mathrm{Gal}(F/K)} h(x) \in \underline{q}_1 \cap \mathcal{O}_K = \underline{p} \subseteq \underline{q}_2$. So for some g, $g(x) \equiv 0 \mod \underline{q}_2$, hence $x \equiv 0 \mod g^{-1}(\underline{q}_2)$. Therefore $g^{-1}(\underline{q}_2) = \underline{q}_1$ by choice of $\underline{x}$. I.e., $\underline{q}_2 = g(\underline{q}_1)$. □

Corollary 2.3. *Let* F/K *be a Galois extension. If* $\underline{q}_1, \underline{q}_2$ *lie above* $\underline{p}$*, then* $e_{\underline{q}_1/\underline{p}} = e_{\underline{q}_2/\underline{p}}$ *and* $f_{\underline{q}_1/\underline{p}} = f_{\underline{q}_2/\underline{p}}$*.*

Hence we can write $e_{\underline{p}}$and $f_{\underline{p}}$ in the case of Galois extensions

Example. Suppose $\mathrm{Gal}(F/K) = S_4$ and $\underline{p}$ splits into $\underline{q}_1, \underline{q}_2, \underline{q}_3, \underline{q}_4$ in F, with the usual action of S_4on 4 elements



Say $H = \{\mathrm{id}, (12)(34)\} \cong C_2$, $L = F^H$. H-orbits of $\left\{\underline{q}_1, \dots, \underline{q}_4\right\}$ are $\left\{\underline{q}_!, \underline{q}_2\right\}$ and $\left\{\underline{q}_3, \underline{q}_4\right\}$, so there exists 2 primes $\underline{r}_1, \underline{r}_2$ in L above $\underline{p}$. ($\underline{r}_1$ splits into $\underline{q}_1$ and $\underline{q}_2$ in F and $\underline{r}_2$ splits into $\underline{q}_3$ and $\underline{q}_4$)

2.2 Decomposition Group

Notation. If $\underline{p}$ is prime of K, write $\mathbb{F}_{\underline{p}} = \mathcal{O}_K/\underline{p}$.

Definition 2.4. Let F/K be a Galois extension of number fields, $\underline{q}$ a prime of F above $\underline{p}$, a prime of K. The *decomposition group* $D_{\underline{q}} = D_{\underline{q}/\underline{p}}$ of $\underline{q}$ (over $\underline{p}$) is $D_{\underline{q}/\underline{p}} = \mathrm{Stab}_{\mathrm{Gal}(F/K)}(\underline{q})$

Remark. $g \in D_{\underline{q}}$ fixes $\underline{q}$ so it acts on $\mathbb{F}_{\underline{q}}$ by $x \mod \underline{q} \mapsto g(x) \mod \underline{q}$. This gives a natural map $D_{\underline{q}} \to \mathrm{Gal}(\mathbb{F}_{\underline{q}}/\mathbb{F}_{\underline{p}})$

Example. Let $K = \mathbb{Q}$, $F = \mathbb{Q}(i)$. Let $p = 3$ and $q = (3)$, complex conjugations fixes $\underline{q}$ and acts as $a + bi \mod (3) \mapsto a - bi \mod 3 = (a+bi)^3 \mod 3$. I.e., exactly as the frobenius automorphism $x \to x^3$ on $\mathbb{F}_{\underline{q}}$.

Theorem 2.5. *Let F/K be a Galois extension of number fields, $\underline{q}$ a prime of F above $\underline{p}$, a prime of K. Then the natural map $D_{\underline{q}} \to \mathrm{Gal}(\mathbb{F}_{\underline{q}}/\mathbb{F}_{\underline{p}})$ is surjective.*

Proof. Pick $\beta \in \mathbb{F}_{\underline{q}}$ such that $\mathbb{F}_{\underline{p}}(\beta) = \mathbb{F}_{\underline{q}}$. Let $f(x) \in \mathbb{F}_{\underline{p}}[x]$ be its minimal polynomial and $\beta = \beta_1, \beta_2, \ldots, \beta_n \in \mathbb{F}_{\underline{q}}$ be its roots (in $\mathbb{F}_{\underline{q}}$ as $\mathbb{F}_{\underline{q}}/\mathbb{F}_{\underline{p}}$ is Galois). Since $g(\beta)$ determines $g \in \mathrm{Gal}(\mathbb{F}_{\underline{q}}/\mathbb{F}_{\underline{p}})$ so is suffices to prove that there exists $g \in D_{\underline{q}}$ with $g(\beta) = g(\beta_2)$.

Pick $\alpha \in \mathcal{O}_K$ with $\alpha \equiv \beta \mod \underline{q}$ and $\alpha \equiv 0 \mod \underline{q}'$ for all other primes $\underline{q}'$ above $\underline{p}$ (possible by CRT Theorem 1.16). Let $F(X) \in \mathcal{O}_K[X]$ be its minimal polynomial over K, and $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m \in \mathcal{O}_F$ be its roots (in F as F/K is Galois). $F(X) \mod \underline{q}$ has β as a root, hence $f(x)$ divides $F(X) \mod \underline{q}$, hence β_2 also is a root of $F(X) \mod \underline{q}$. Without loss of generality $\alpha_2 \mod \underline{q} = \beta_2$. Take $g \in \mathrm{Gal}(F/K)$ with $g(\alpha) = \alpha_2$. Then $g(\alpha) \neq 0 \mod \underline{q}$, hence $g(\underline{q}) = \underline{q}$ so $g \in D_{\underline{q}}$, and $g(\beta) = \beta_2$ ☐

Corollary 2.6. *Let K be a number field, F/K the splitting field of a monic irreducible $f(x) \in \mathcal{O}_K[x]$, of degree n. Suppose for some prime $\underline{p}$ of K, $f(x) \mod \underline{p} = g_1(x)g_2(x)\ldots g_k(x)$ with $g_i(x) \in \mathbb{F}_{\underline{p}}[x]$ be distinct irreducible with $\deg g_i = d_i$. Then $\mathrm{Gal}(F/K) \subseteq S_n$ contains an element of cycle type $(d_1, d_2, \ldots, d_k)$*

Proof. Let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ be the roots of $f(x)$. Then $\beta_i = \alpha_i \mod \underline{q}$ ($\underline{q}$ any prime above $\underline{p}$) are precisely the roots of $f(x) \mod \underline{p}$ in $\mathbb{F}_{\underline{q}}$. Their generator of $\mathrm{Gal}(\mathbb{F}_{\underline{q}}/\mathbb{F}_{\underline{p}})$ permutes the β_i with cycle type $(d_1, \ldots, d_k)$. Hence its lift to $D_{\underline{q}} \leq \mathrm{Gal}(F/K)$ has the claimed cycle type. ☐

Definition 2.7. Let F/K be Galois, $\underline{q}$ a prime above $\underline{p}$. The *inertia subgroup* $I_{\underline{q}} = I_{\underline{q}/\underline{p}}$ is the (normal) subgroup of $D_{\underline{q}}$ that acts trivially on $\mathbb{F}_{\underline{q}}$, i.e., $I_{\underline{q}} = \ker(D_{\underline{q}} \to \mathrm{Gal}(\mathbb{F}_{\underline{q}}/\mathbb{F}_{\underline{p}}))$.

Note that as the amp is surjective $D_{\underline{q}}/I_{\underline{q}} \cong \mathrm{Gal}(\mathbb{F}_{\underline{q}}/\mathbb{F}_{\underline{p}})$. The latter group is cyclic and is generated by the frobenius map $\phi : x \to x^{\#\mathbb{F}_{\underline{p}}}$.

Definition 2.8. The (arithmetic) *Frobenius element* $\mathrm{Frob}_{\underline{q}/\underline{p}}$ is the element of $D_{\underline{q}}/I_{\underline{q}}$ that maps to ϕ.

Theorem 2.9. *Let F/K be Galois extensions of number field, $\underline{q}$ a prime of F above $\underline{p}$, a prime of K. Then*

1. $\left|D_{\underline{q}/\underline{p}}\right| = e_{\underline{q}/\underline{p}} \cdot f_{\underline{q}/\underline{p}}$
2. *Order of* $\mathrm{Frob}_{\underline{q}/\underline{p}}$ *is* $f_{\underline{q}/\underline{p}}$
3. $\left|I_{\underline{q}/\underline{p}}\right| = e_{\underline{q}/\underline{p}}$

If $K \leq L \leq F$ and $\underline{s}$ is above $\underline{p}$, below $\underline{q}$

4. $D_{\underline{q}/\underline{s}} = D_{\underline{q}/\underline{p}} \cap \mathrm{Gal}(F/L)$
5. $I_{\underline{q}/\underline{s}} = I_{\underline{q}/\underline{p}} \cap \mathrm{Gal}(F/L)$

Proof.

1. Let $n = \#\text{primes above } \underline{p}$. Then

$$\begin{aligned} n \cdot \left|D_{\underline{q}/\underline{p}}\right| &= |\mathrm{Gal}(F/K)| \ \ (\text{orbit} - \text{stabiliser}) \\ &= [F:K] \\ &= \sum e_i f_i \ \ (\text{Theorem } 1.26) \\ &= n e_{\underline{q}/\underline{p}} f_{\underline{q}/\underline{p}} \end{aligned}$$

2. $f_{\underline{q}/\underline{p}} = [\mathbb{F}_{\underline{q}} : \mathbb{F}_{\underline{p}}] = \left|\mathrm{Gal}(\mathbb{F}_{\underline{q}}/\mathbb{F}_{\underline{p}})\right|$ =order of $\mathrm{Frob}_{\underline{q}/\underline{p}}$

3. $\left|D_{\underline{q}/\underline{p}}\right| = \left|I_{\underline{q}/\underline{p}}\right|$ ·order of $\mathrm{Frob}_{\underline{q}/\underline{p}}$, hence $\left|I_{\underline{q}/\underline{p}}\right| = e_{\underline{q}/\underline{p}}$

4. and 5. Just from definition.

$\square$

Example.

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) = F \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, no head] & \mathbb{Q}(\sqrt{3}) \arrow[d, no head] & \mathbb{Q}(\sqrt{6}) \arrow[dl, no head] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Now 2 ramifies in all three quadratic fields:

- $(2) = \left(\sqrt{2}\right)^2$
- $(x^2 - 3) = (x+1)^2 \mod 2$
- $(x^2 - 6) = x^2 \mod 2$

and use Kummer - Dedekind. Let $\underline{q}$ in F, hence $e \geq 2$, so $\left|I_{\underline{q}}\right| \geq 2$, so $I_{\underline{q}}$ contains $\mathrm{Gal}(F/\mathbb{Q}\left(\sqrt{d}\right))$ for some d. So the prime above 2 in $F/\mathbb{Q}(\sqrt{d})$ is ramified, so $e_{\underline{q}} = 2 \cdot 2 = 4$ and $I_{\underline{q}} = C_2 \times C_2$.

Example. Let $K = \mathbb{Q}$, $F = \mathbb{Q}(\zeta_n)$. Let $p \nmid n$ be a prime, $\underline{q}$ a prime of F above $\underline{p}$. We know that $\underline{p}$ is unramified, so $I_{\underline{q}/\underline{p}} = \{\mathrm{id}\}$ and $D_{\underline{q}/\underline{p}} = \left\langle \mathrm{Frob}_{\underline{q}/\underline{p}} \right\rangle$. Now $\mathrm{Frob}_{\underline{q}/\underline{p}}(\zeta_n) \equiv \zeta_n^p \mod \underline{q}$ and hence $\mathrm{Frob}_{\underline{q}/\underline{p}}(\zeta_n) = \zeta_n^p$ as ζ_n^i are distinct in $\mathbb{F}_{\underline{q}}$. (Since $x^n - 1 \mod \underline{p}$ has distinct roots). In particular, $e_{\underline{q}/\underline{p}} = 1$ and $f_{\underline{q}/\underline{p}}$ =order of $\mathrm{Frob}_{\underline{q}/\underline{p}}$ =order of p in $(\mathbb{Z}/n\mathbb{Z})^*$.

2.3 Counting primes

Lemma 2.10. *Let F/K be a Galois extension of number fields.*

1. *primes of K are in 1-1 correspondence with $\mathrm{Gal}(F/K)$-orbits on primes of F via $\underline{p} \leftrightarrow$primes of F above $\underline{p}$.*
2. *If $\underline{q}$ lies above $\underline{p}$ then $gD_{\underline{q}} \mapsto g(\underline{q})$ is a $\mathrm{Gal}(F/K)$ set isomorphism from $\{\text{primes above } \underline{p}\}$ to $G/D_{\underline{q}}$*
3. *$D_{g(\underline{q})} = gD_{\underline{q}}g^{-1}$, $I_{g(\underline{q})} = gI_{\underline{q}}g^{-1}$ and $\mathrm{Frob}_{g(\underline{q})/\underline{p}} = g\mathrm{Frob}_{\underline{q}/\underline{p}}g^{-1}$.*

Proof. 1. is from transitivity of the Galois action while 2. and 3. are elementary check $\square$

Corollary 2.11. *Let F/K be Galois, $K \leq L \leq F$, $G = \mathrm{Gal}(F/K), H = \mathrm{Gal}(F/L)$. Then*

$$\{\text{primes of } L \text{ above } \underline{p}\} \leftrightarrow H\text{−orbits on primes of } F \textit{ above } \underline{p} \leftrightarrow H\backslash G/D_{\underline{q}} = \{HgD_{\underline{q}}\}$$

via $\underline{s} \mapsto$elements that sent $\underline{q}$ to some prime above $\underline{s}$.

Proposition 2.12. *Let F/K be Galois extension of number fields, $L = K(\alpha)$ an intermediate field, $G = \mathrm{Gal}(F/K)$ and $H = \mathrm{Gal}(F/L)$. Let $X = \{\text{roots of min poly of } \alpha\} \cong \{\text{embeddings } L \hookrightarrow F\} = H\backslash G$ a G-set of size $[L : F]$.*

Then $\{\text{primes of } L \text{ above } \underline{p}\} \overset{1:1}{\leftrightarrow} D_{\underline{q}}$-orbits on X with

- size $D_{\underline{q}}$-orbits$= e_{\underline{s}/\underline{p}} \cdot f_{\underline{s}/\underline{p}}$
- size $I_{\underline{q}}$-suborbits $= e_{\underline{s}/\underline{p}}$
- number $I_{\underline{q}}$-suborbits$= f_{\underline{s}/\underline{p}}$

Explicitly, $\underline{s} \mapsto$Orbits of $g^{-1}(\alpha)$ *where* $g(\underline{q})$ *lies above* $\underline{s}$.

Example. Let $K=\mathbb{Q}$, $F=\mathbb{Q}(\zeta_5, \sqrt[5]{2})$, $p=73$, Let $\underline{q}$ be a prime of F above $\underline{p}$

$$\begin{tikzcd}
 & F \arrow[dl, dash] \arrow[dd, dash] \\
L=\mathbb{Q}(\sqrt[5]{2}) \arrow[dr, dash] & \\
 & \mathbb{Q}
\end{tikzcd}$$

Now $\underline{p}$ is unramified in F with residue degree 4 (use Kummer - Dedekind on $L/\mathbb{Q}$ and $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ and that $\mathrm{Gal}(F/\mathbb{Q})$ has no element of order 20). Now $\mathrm{Gal}(F/\mathbb{Q})$ permutes $\sqrt[5]{2}, \zeta\sqrt[5]{2}, \dots$ transitively, $e_{\underline{q}/73}=1$, hence $I_{\underline{q}}$-orbits are trivial. $f_{\underline{q}}=4$ hence $\left|D_{\underline{q}}\right|=4$, $D_{\underline{q}} \cong C_4$ (generated by Frob). Without loss of generality $D_{\underline{q}}$ fixes $\sqrt[5]{2}$ and permutes the rest cyclically. Hence there are 2 primes in L above 73 with residue degree 1 and 4 and ramification degrees 1 and 1.

Proof of Theorem 2.12. We have

$$\begin{aligned}
\{\text{primes of } L \text{ above } p\} &\leftrightarrow H\backslash G/D_{\underline{q}} \\
&\leftrightarrow D_{\underline{q}}-\text{orbits on } H\backslash G =: X
\end{aligned}$$

($D_{\underline{q}}$ acts by $d(Hg)=Hgd^{-1}$). Size of $D_{\underline{q}}$-orbits of

$$\begin{aligned}
g^{-1}(\alpha) &= \frac{\left|D_{\underline{q}}\right|}{\left|\mathrm{Stab}_{D_{\underline{q}}}(g^{-1}(\alpha))\right|} \\
&= \frac{\left|D_{\underline{q}}\right|}{\left|\mathrm{Stab}_{gD_{\underline{q}}g^{-1}}(\alpha)\right|} \\
&= \frac{\left|D_{\underline{q}}\right|}{|gDg^{-1}\cap H|} \\
&= \frac{\left|D_{\underline{q}}\right|}{\left|D_{g(\underline{q})/\underline{p}}\right|} \\
&= \frac{e_{\underline{q}/\underline{p}} \cdot f_{\underline{q}/\underline{p}}}{e_{\underline{q}/\underline{s}} \cdot f_{\underline{q}/\underline{s}}} \\
&= e_{\underline{s}/\underline{p}} \cdot f_{\underline{s}/\underline{p}}
\end{aligned}$$

Similarly, size of $I_{\underline{q}}$-orbits is $e_{\underline{s}/\underline{p}}$ (same calculations as above, replacing $D_{\underline{q}}$ with $I_{\underline{q}}$). And hence $\#I_{\underline{q}}$ -suborbits is $\frac{e_{\underline{s}/\underline{p}} \cdot f_{\underline{s}/\underline{p}}}{e_{\underline{s}/\underline{p}}} = f_{\underline{s}/\underline{p}}$. $\square$

2.4 Representation of the decomposition group

Let F/K be a Galois Extensions of number fields. Let $G = \mathrm{Gal}(F/K)$, $\underline{p}$ a prime in $\mathcal{O}_K$, $\underline{q}$ a prime above $\underline{p}$ in $\mathcal{O}_F$. Let $D = D_{\underline{q}/\underline{p}}$ and $I = I_{\underline{q}/\underline{p}}$, $\mathrm{Frob} = \mathrm{Frob}_{\underline{q}/\underline{p}}$.

Definition 2.13. A representation V of D is *unramified* if I acts trivially on V, therefore $V^I = V$ (F/K is unramified if and only if all V are unramified)

Notation. For a $f_{\underline{q}/\underline{p}}^{\mathrm{th}}$-root of unity ζ, define the representation $\Psi_{\underline{q}/\underline{p},\zeta} = \Psi_\zeta : D \to \mathbb{C}^* = \mathrm{GL}_1(\mathbb{C})$ such that $\Psi_\zeta(h) = 1$ $(h \in I)$, $\Psi_\zeta(\mathrm{Frob}) = \zeta$. Thus $\Psi_\zeta(g) = \zeta^k$ if g acts as $x \mapsto x^{(\#\mathbb{F}_{\underline{p}})^k}$ on $\mathbb{F}_{\underline{q}}$.

Lemma 2.14. *If V is a irreducible representation of D then either $V^I = 0$ or V is unramified and $V = \Psi_\zeta$ for some ζ with $\zeta^{f_{\underline{q}/\underline{p}}} = 1$.*

Proof. Since $I \lhd D$ it follows that V^I is a subrepresentation of V. Then either $V^I = 0$ or $V^I = V$.In the latter case, the action of D factors through $D/I = \langle \mathrm{Frob} \rangle$ and hence V is 1-dimensional and $V = \Psi_\zeta$ for some ζ. $\square$

Notation. If $\underline{q}' = g(\underline{q})$ is another prime above $\underline{p}$ for some $g \in G$ and (ρ, V) a representation of D, we write (ρ^g, V^g) for the corresponding representation of $D_{\underline{q}//\underline{p}}$ given by $\rho^g(h) = \rho(ghg^{-1})$. Clearly $D_{\underline{q}/\underline{p}} \cong D_{\underline{q}'/\underline{p}}$ as groups.

Example. Let $G \cong S_4$, $D = D_8$ and $I = C_4$. Then there are $|G/D|$-prime above $\underline{p}$. $D_8 \cong D_{\underline{q}/\underline{p}}$. Others are the two other subgroup of S_4 isomorphic to D_8.

D_8	e	(1234)	$(13)(24)$	$(12)(34)$	(13)
1	1	1	1	1	1
ϵ_1	1	1	1	-1	1
ϵ_2	1	-1	1	1	-1
ϵ_3	1	-1	1	-1	1
ρ	2	0	-2	0	0

The 2-dimensional irreducible representation of $D_{\underline{q}'/\underline{p}}$ is obtained as $\rho'(h) = \rho(g^{-1}hg)$.

Lemma 2.15.

1. *If $\underline{q}' = g(\underline{q})$ another prime over $\underline{p}$ then $\Psi_{\underline{q}'/\underline{p},\zeta} = \Psi^g_{\underline{q}/\underline{p},\zeta}$*
2. *If L is an intermediate field, Σ is a prime below $\underline{q}$ then $\mathrm{Res}_{D_{\underline{q}/\Sigma}} \Psi_\zeta = \Psi_{\underline{q}/\Sigma,\zeta^f}$ whence $f = f_{\Sigma/\underline{p}}$. In particular $\mathrm{Res}_{D_{\underline{q}/\Sigma}} \Psi_{\underline{q}/\underline{p},\zeta} = \mathbb{I} \iff \zeta^{f_{\Sigma/\underline{p}}} = 1$*

Proof.

1. Follows from $D_{\underline{q}'/\underline{p}} = gDg^{-1}$, $I_{\underline{q}'/\underline{p}} = gIg^{-1}$ and $\mathrm{Frob}_{\underline{q}'/\underline{p}} = g\mathrm{Frob}g^{-1}$
2. $\mathrm{Res}_{D_{\underline{q}/\Sigma}} \Psi_{\underline{q}/\underline{p},\zeta}$ sends $I_{\underline{q}/\Sigma}$ to 1 and $\mathrm{Frob}_{\underline{q}/\Sigma}$ to ζ^f because $\mathrm{Frob}_{\underline{q}/\Sigma}$ acts as $x \to x^{(\#\mathbb{F}_{\underline{p}})^f}$ on $\mathbb{F}_{\underline{q}}$.

$\square$

Proposition 2.16. *Let $K \subseteq L \subseteq F$, $H = \mathrm{Gal}(F/L)$*

$$\begin{tikzcd}
\underline{q}_i \arrow[d, dash] & - \arrow[dd, dash, "G"] & F \arrow[d, dash] & - \arrow[d, dash, "H"'] \\
\Sigma \arrow[d, dash] & & L \arrow[d, dash] & - \\
\underline{p} & - & K &
\end{tikzcd}$$

Let $\{\Sigma_i\}$ be the set of primes of L above $\underline{p}$ and pick $\underline{q}_i = g_i(\underline{q})$ above Σ_i for each i. For V a representation of H

$$\mathrm{Res}_D^G \mathrm{Ind}_H^G V \cong \bigoplus_{\Sigma_i} \left(\mathrm{Ind}_{D_{\underline{q}_i/\Sigma_i}}^{D_{\underline{q}_i/\underline{p}}} \mathrm{Res}_{D_{\underline{q}_i/\Sigma_i}}^H V \right)^{g_i^{-1}}.$$

In particular

$$\left\langle \Psi_\zeta, \mathrm{Res}_D \mathrm{Ind}_H^G V \right\rangle = \sum_{\Sigma_i} \left\langle \Psi_{\underline{q}_i/\Sigma_i, \rho^{f_{\Sigma_i/\underline{p}}}}, \mathrm{Res}_{D_{\underline{q}_i,\Sigma_i}} V \right\rangle.$$

Proof. The main claim is precisely Mackey's formula for $H, D \leq G$. The second claim then follows from

$$\begin{aligned}
\left\langle \Psi_\zeta, (\mathrm{IndRes} V)^{g_i^{-1}} \right\rangle_{D_{\underline{q}/\underline{p}}} &= \left\langle \Psi_{\underline{q}_i/\underline{p},\zeta}, \mathrm{IndRes} V \right\rangle_{D_{\underline{q}_i/\underline{p}}} \\
&= \left\langle \mathrm{Res}\Psi_{\underline{q}_i/\underline{p},\zeta}, \mathrm{Res} V \right\rangle_{D_{\underline{q}_i/\Sigma_i}} \text{ by Frobenius reciprocity} \\
&= \left\langle \Psi_{\underline{q}_i/\Sigma_i, \zeta^{f_{\Sigma_i/\underline{p}}}}, \mathrm{Res} V \right\rangle
\end{aligned}$$

□

Corollary 2.17. *Let ζ be a primitive n^{th} root of unity with $n | f_{\underline{q}/\underline{p}}$. Then $K \subseteq L \subseteq F$ with $H = \mathrm{Gal}(F/L)$. The number of primes of L above $\underline{p} = \left\langle \Psi_\zeta, \mathrm{Res}_D^G \mathrm{Ind}_J^G \mathbb{I} \right\rangle$*

Proof. By previous proposition, the Right Hand Side is $\sum_{\Sigma \text{ above } \underline{p}} \left\langle \Psi_{\underline{q}'/\Sigma', \zeta^{f_{\Sigma/\underline{p}}}}, \mathbb{I} \right\rangle = \#\Sigma$ with $\zeta^{f_{\Sigma/\underline{p}}} = 1$ □

3 L-series

Aim:

1. If $\gcd(a, n) = 1$ then there are infinitely many primes $p \equiv a \mod n$
2. If $f(x) \in \mathbb{Z}[x]$ monic and $f(x) \mod p$ has a root $\mod p$ for all p, then $f(x)$ is reducible.

Definition 3.1. An *ordinary Dirichlet series* is a series $f(s) = \sum_{s=1}^{\infty} a_n n^{-s}$ $(a_n \in \mathbb{C}, s \in \mathbb{C})$.

Convention: $s = \sigma + it$.

Convergence Property

Lemma 3.2 (Abel's Lemma)**.** $\sum_{n=N}^{M} a_n b_n = \sum_{n=N}^{M-1} \left(\sum_{k=N}^{n} a_k\right)(b_n - b_{n+1}) + \left(\sum_{k=N}^{M} a_k\right) b_M$

Proof. Elementary rearrangement (c.f., integration by part) □

Proposition 3.3. *Let $f(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$ for $\lambda_n \to \infty$ an increasing sequence of the real number*

1. *If the partial sums $\sum_N^M a_n$ are bounded, then the series converges locally uniformly of* $\mathrm{Re}(s) > 0$ *to an analytic functions*
2. *If the series $f(s)$ converges for $s = s_0$, then it converges uniformly on* $\mathrm{Re}(s) > \mathrm{Re}(s_0)$ *to an analytic function.*

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

Proof. Note that 1. implies 2. by the change of variables $s' = s - s_0$ and $a'_n = e^{-\lambda_n s_0} a_n$. The new series converges at 0 and so must have $\sum_N^M a'_n$ bounded

For 1. we will show uniform convergence on $-A < \arg(s) < A$ and $\mathrm{Re}(s) > \delta$. This will suffice as the uniform limit of analytic functions is analytic and these regions cover $\mathrm{Re}(s) > 0$.

Let $\epsilon > 0$, find N_0 such that $n > N_0$, $\left|e^{-\lambda_n s}\right| < \epsilon$ in this domain. Now compute: for $N_1 M \geq N_0$

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

where B is the bound for the partial sums.

Observe:

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

where $\sigma = \mathrm{Re}(s)$ for $\alpha > \beta$. So

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

where $\left|\frac{s}{\sigma}\right| \leq K$ in our domain. □

Proposition 3.4. *Let $f(s) = \sum a_n e^{-\lambda_n s}$ for $\lambda_n \to \infty$ an increasing sequence of positive reals. Suppose*

- *$a_n \geq 0$ is real*
- *$f(s)$ converges on $\mathrm{Re}(s) > R$ ($\in \mathbb{R}$) and hence is analytic*
- *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 can assume $R = 0$. As f is analytic on $\mathrm{Re}(s) > 0$ and $|s| < \delta$. Hence f is 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 $f(-\epsilon) = \sum_{k=0}^{\infty}\frac{1}{k!}(-1)^k(1+\epsilon)^k f^{(k)}(1)$ converges. For $\mathrm{Re}(s) > 0$ $f^{(k)}(s) = \sum_{n=1}^{\infty} a_n(-\lambda_n)^k e^{-\lambda_n}$ (ok since uniform convergence). Hence $(-1)f^{(k)}(s) = \sum_{n=1}^{\infty} a_n \lambda_n^k e^{-\lambda_n}$. Hence

$$\begin{aligned}
f(-\epsilon) &= \sum_{k=0}^{\infty} \frac{1}{k!}(1+\epsilon)^k \sum_{n=1}^{\infty} a_n \lambda_n^k e^{-\lambda_n} \\
&= \sum_{k,n} a_n \lambda_n^k e^{-\lambda_n} e^{-\lambda_n} \frac{1}{k!}(1+\epsilon)^k \text{ as all terms positive} \\
&= \sum_{n=1}^{\infty} a_n e^{-\lambda_n} e^{-\lambda_n(1+\epsilon)} \\
&= \sum_{n=1}^{\infty} a_n e^{\lambda_n \epsilon}
\end{aligned}$$

is a convergent series for f converges at $s = -\epsilon$. This implies the result. □

Theorem 3.5.

1. *If a_n are bounded, then $\sum_{n\geq 1} a_n n^{-s}$ converges absolutely on* $\mathrm{Re}(s) > 1$ *to an analytic function.*
2. *If the partial sums $\sum_N^M a_n$ are bounded then $\sum a_n n^{-s}$ converges absolutely on* $\mathrm{Re}(s) > 0$ *to an analytic function.*

Proof.

1. $\left|\frac{a_n}{n^s}\right| \leq k\frac{1}{n^\sigma}$ where $\sigma = \mathrm{Re}(s)$ and $\sum_{n=1}^{\infty} \frac{1}{n^x}$ does converge for $x > 1$ real. Analytic comes from Proposition 3.3
2. See Proposition 3.3

□

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

3.1 Dirichlet L-functions

Definition 3.6. Let $N \geq 1$ be an integer $\psi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ a group homomorphism. Extend ψ to a function on $\mathbb{Z}$ by $\psi(n) = \begin{cases} \psi(n \mod N) & \gcd(n,N) = 1 \\ 0 & \text{else} \end{cases}$. Such a function is called a *Dirichlet character modulo N.*

Its *L-series* (or *L-function*) is $L_N(\psi, s) = \sum_{n=1}^{\infty} \psi(n) n^{-s}$.

Lemma 3.7. *Let ψ be a Dirichlet character modulo N. Then*

1. *$\psi(a+N) = \psi(a)$ (so ψ is periodic)*
2. *$\psi(ab) = \psi(a)\psi(b)$ (so ψ is strictly multiplicative)*
3. *The L-series for ψ converges absolutely on* $\mathrm{Re}(s) > 1$ *and satisfies the* Euler product
$$L_n(\psi, s) = \prod_{p \text{ prime}} \frac{1}{1 - \psi(p)p^{-s}}.$$

Proof. 1. and 2. are clear from the definition. 3. the L-series coefficients $a_n = \psi(n)$ are bounded, so absolute convergence follows from Theorem 3.5. For $\mathrm{Re}(s) > 1$

$$\begin{aligned}
\sum \psi(n) n^{-1} &= \prod_{p \text{ prime}} (1 + \psi(p)p^{-s} + \psi(p)^2 p^{-2s} + \dots) \text{ (by 2. and abs conv)} \\
&= \prod_{p \text{ prime}} \frac{1}{1 - \psi(p)p^{-s}} \text{ (geometric series)}
\end{aligned}$$

□

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

$$\begin{aligned} L_N(\psi, s) &= \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} \\ &= \zeta(s) \cdot \prod_{p|N, \text{ prime}} (1 - p^{-s}) \end{aligned}$$

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

Example. Take $N = 10$, so $(\mathbb{Z}/N\mathbb{Z})^* = \{1, 3, 7, 9\} \cong C_4$, and $\psi(1) = 1$, $\psi(3) = i$, $\psi(7) = -i$ and $\psi(9) = -1$. Then $L_{10}(\psi, s) = 1 + \frac{i}{3^s} - \frac{i}{7^s} - \frac{1}{11^s} + \frac{1}{11^s} + \frac{i}{13^s} - \frac{i}{17^s} - \frac{1}{19^s} + \dots$. Note that by the alternating series test (applied to the real part and imaginary part separately) implies convergence on $s > 0$ real.

Theorem 3.8. *Let $N \geq 1$ and $\psi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$.*

1. *If ψ is trivial then $L_N(\psi, s)$ has an analytic continuation to $\mathrm{Re}(s) > 0$ except for a simple pole at $s = 1$*
2. *If ψ is non-trivial, then $L_N(\psi, s)$ is analytic on $\mathrm{Re}(s) > 0$*

Proof.

1. Follows from the previous remark and that $\zeta(s)$ has an analytic continuation to $\mathrm{Re}(s) > 0$ with a simple pole at $s = 1$.
2. $\sum_{n=A}^{A+N-1} \psi(n) = \sum_{n \in (\mathbb{Z}/N\mathbb{Z})^*} \psi(n) \cdot \overline{1} = \psi(N) \langle \psi, \mathbb{I} \rangle = 0$ as $\psi \neq 1$. So the partial sums $\sum_A^B \psi(n)$ are bounded and the result follows from Theorem 3.5ii)

□

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

Proof. Let

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

If $L_N(\psi, 1) = 0$ then $\zeta_N(s)$ has an analytic continuation to $\mathrm{Re}(s) > 0$, the pole form $L_N(\mathbb{I}, s)$ having been killed by the zero on $L_N(\psi, s)$. We'll show that this is not the case (and hence has a simple pole at $s = 1$)

On $\mathrm{Re}(s) > 1$, $\zeta_N(s)$ has the absolutely convergent expression

$$\begin{aligned} \zeta_N(s) &= \prod_{\chi} \prod_{p \nmid N} \frac{1}{1 - \chi(p) p^{-s}} \\ &= \prod_{p \nmid N} \prod_{\chi} \frac{1}{1 - \chi(p) p^{-s}} \\ &= \prod_{p \nmid N} \frac{1}{(1 - p^{-f_p s})^{\phi(N)/f_p}} \end{aligned}$$

where ϕ is the Euler totient function and f_p the order of p in $(\mathbb{Z}/N\mathbb{Z})^*$. Hence

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

This is a Dirichlet series with positive real coefficient so if it has an analytic continuation to $\mathrm{Re}(s) > 0$, it must converge there by Proposition 3.4. But for $s > 0$ real it dominates

$$\prod_{p \nmid N} (1 + p^{-\phi(N)s} + p^{-2\phi(N)s} + \dots) = L_N(\mathbb{I}, \phi(N)s)$$

which diverges for $s = 1/\phi(N)$. □

3.2 Primes in Arithmetic Progression

Strategy: $\sum_{p\equiv a \mod N} p^{-s} = \sum_\chi \lambda_\chi \sum_p \chi(p)p^{-s}$ with $\lambda_{\mathbb{I}} \neq 0$. This is approximately $\sum_\chi \lambda_\chi \log L_N(\chi, s) \sim \lambda_{\mathbb{I}} \log \frac{1}{s-1} \to \infty$ as $s \to 1$.

Proposition 3.10. *Let ψ be a Dirichlet character modulo N*

1. *The Dirichlet series $\sum_{p \text{ prime}, n\geq 2} \frac{\psi(p)^n}{n} p^{-ns}$ converges on $\mathrm{Re}(s) > 1$ so it is an analytic function and defines (a branch of) $\log L_N(\psi, s)$ there.*
2. *If ψ is non-trivial then $\sum_{p,n} \frac{\psi(p)^n}{n} p^{-ns}$ is bounded as $s \to 1$. If $\psi = \mathbb{I}$ then $\sum_{p,n} \frac{1}{n} p^{-ns} \sim \log \frac{1}{1-s}$ as $s \to 1$.*

Proof.

1. The series has bounded coefficients so converges absolutely on $\mathrm{Re}(s) > 1$ to an analytic function by Theorem 3.5 1. For a fixed s with $\mathrm{Re}(s) > 1$

$$\begin{aligned}
\sum_{p,n} \frac{\psi(p)^n}{n} p^{-ns} &= \sum_p \left(\psi(p)p^{-s} + \frac{(\psi(p)p^{-s})^2}{2} + \dots \right) \\
&= \sum_p \log \frac{1}{1-\psi(p)p^{-s}} \text{ (branch with } \log(1+x) = x - \frac{x^2}{2} + \dots) \\
&= \log \prod_p \frac{1}{1-\psi(p)p^{-s}} \text{ (possibly a diff branch)} \\
&= \log L_N(\psi, s)
\end{aligned}$$

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

2. By Theorem 3.8, for $\psi \neq \mathbb{I}$, $L_N(\psi, s)$ converges to a non-zero value as $s \to 1$, so $\log L_N(\psi, s)$ is bounded as $s \to 1$. For $L_N(\mathbb{I}, s)$ has a simple pole at $s = 1$ (hence $\sim \frac{\lambda}{s-1}$) so $\log L_N(\mathbb{I}, s) \sim \log \frac{1}{s-1}$ as $s \to 1$.

□

Corollary 3.11. *If ψ is non-trivial then $\sum_{p \text{ prime}} \psi(p)p^{-s}$ is bounded as $s \to 1$. If $\psi = \mathbb{I}$, then $\sum_{p \text{ prime}} \psi(p)p^{-s} = \sum_{p\nmid N} p^{-s} \sim \log \frac{1}{s-1}$ as $s \to 1$ and in particular tends to ∞ as $s \to 1$.*

Proof. $\sum_p \psi(p)p^{-s} = \log L_N(\psi, s) - \sum_{p,n\geq 2} \frac{\psi(p)^n}{n} p^{-ns}$ so it suffices to check that the last term is bounded on $\mathrm{Re}(s) > 1$.

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

□

Dirichlet's Theorem on primes in Arithmetic Progression. *Let a, N be coprime integers. Then there are infinitely many primes $p \equiv a \mod N$. Moreover if $P_{a,N}$ is the set of these primes then $\sum_{p\in P_{a,N}} \frac{1}{p^{-s}} \sim \frac{1}{\phi(N)} \log \frac{1}{s-1}$ as $s \to 1$.*

Proof. The first statement follows from the second as $\log \frac{1}{s-1} \to \infty$ as $s \to 1$. Consider the (class-)function $\mathcal{C}_{a,N} : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ with $C_{a,N}(n) = \begin{cases} 1 & \text{if } n = a \\ 0 & \text{else} \end{cases}$. Then

$$\begin{aligned} \langle \mathcal{C}_{a,N}, \chi \rangle &= \frac{1}{\phi(N)} \sum_{n \in (\mathbb{Z}/N\mathbb{Z})^*} C_{a,N}(n)\overline{\chi(n)} \\ &= \frac{1}{\phi(N)} \overline{\chi(a)} \end{aligned}$$

so $C_{a,n} = \sum_\chi \frac{\overline{\chi(a)}}{\phi(N)} \chi$ by Character theory. Hence

$$\begin{aligned} \sum_{p \in P_{a,N}} \frac{1}{p^s} &= \sum_{p \text{ prime}} C_{a,n}(p) p^{-s} \\ &= \sum \frac{\overline{\chi(a)}}{\psi(N)} \sum_p \frac{\chi(p)}{p^s} \end{aligned}$$

By Corollary 3.11, each term on RHS is bounded as $s \to 1$ except for $\chi = \mathbb{I}$, and

$$\begin{aligned} \frac{\mathbb{I}}{\phi(N)} \sum \frac{\mathbb{I}(p)}{p^s} &= \frac{1}{\phi(N)} \sum_{p \nmid N} \frac{1}{p^s} \\ &\sim \frac{1}{\phi(N)} \log \frac{1}{s-1} \end{aligned}$$

as $s \to 1$. □

3.3 Artin L-functions

Definition 3.12. Let F/K be a Galois extension of number fields and ρ a $\mathrm{Gal}(F/K)$-represnetation. The *Artin L-function of* ρ is defined by the Euler product

$$\begin{aligned} L(F/K, \rho, s) &= L(\rho, s) \\ &= \prod_{\underline{p} \text{ prime of } K} \frac{1}{P_{\underline{p}}(\rho, N(\underline{p})^{-s})} \end{aligned}$$

where the *local polynomial* of ρ at $\underline{p}$, $P_{\underline{p}}(\rho, T)$ is defined by $P_{\underline{p}}(\rho, T) = \det(1 - \mathrm{Frob}_{\underline{p}} T | \rho^{I_{\underline{p}}})$. ($= \det(I - MT)$ where M is the matrix by which $\mathrm{Frob}_{\underline{p}}$ acts on $\rho^{I_{\underline{p}}}$). Note that here $I_{\underline{p}} = I_{\underline{q}/\underline{p}}$ and $\mathrm{Frob}_{\underline{p}} = \mathrm{Frob}_{\underline{q}/\underline{p}}$ for some (Any) prime $\underline{q}$ above $\underline{p}$.

Example.

- Take $K = \mathbb{Q}$, F arbitrary, $\rho = \mathbb{I}$. Then $P_{\underline{p}}(\mathbb{I}, t) = \det(1 - 1 \cdot t) = 1 - t$ for all $\underline{p}$. Hence $L(\mathbb{I}, s) = \prod_p \frac{1}{1-p^{-s}} = \zeta(s)$.
- Similarly, for general K and $\rho = \mathbb{I}$ we get $P_{\underline{p}}(\mathbb{I}, t) = 1 - t \forall \underline{p}$. Then $L(F/K, \mathbb{I}, s) = \prod_{\underline{p}} \frac{1}{1 - N(\underline{p})^{-s}} = \zeta_K(s)$ (The *Dedekind ζ-function of K*)
- $K = \mathbb{Q}$,$F = \mathbb{Q}(i)$, $\rho : \mathrm{Gal}(F/K) = C_2 \to \{\pm 1\}$ non-trivial 1-dimensional representation. Then

  $$P_{\underline{p}}(\rho, T) = \begin{cases} 1 & \underline{p} = 2 \Rightarrow \rho^{I_{\underline{p}}} = 0 \\ 1 - t & p \equiv 1 \mod 4 \Rightarrow \mathrm{Frob}_{\underline{p}} = \mathrm{id} \\ 1 + t & p \equiv 3 \mod 4 \Rightarrow \mathrm{Frob}_{\underline{p}} \neq \mathrm{id} \end{cases}$$

  Hence $L(\rho, s) = \prod_{p \equiv 1 \mod 4} \frac{1}{1-p^{-s}} \prod_{p \equiv 3 \mod 4} \frac{1}{1+p^{-s}} = \prod_p \frac{1}{1 - \chi(p) p^{-s}}$ where $\chi : \mathbb{Z} \to \mathbb{C}^*$ is the non-trivial Dirichlet character mod 4. That is $L(\rho, s) = L_4(\chi, s)$ a Dirichlet L-function.

Lemma 3.13. *The local polynomial $P_{\underline{p}}(\rho, T)$ is independent of the choice of $\underline{q}$ above $\underline{p}$ and of the choice of* $\mathrm{Frob}_{\underline{p}}$.

Proof. For a fixed $\underline{q}$ above $\underline{p}$, independence of the choice of $\mathrm{Frob}_{\underline{p}}$ is clear. Since two choices differ by an element $\sigma \in I_{\underline{p}}$, which acts trivially on $\rho^{I_{\underline{p}}}$. Hence $\det(1 - \mathrm{Frob}_{\underline{p}} t | \rho^{I_{\underline{p}}}) = \det(1 - \sigma \mathrm{Frob}_{\underline{p}} t | \rho^{I_{\underline{p}}})$.

If $\underline{q}' = g(\underline{q})$ is another prime above $\underline{p}$, then the matrix of $\rho(d)$ for $d \in \mathrm{Gal}(F/K)$ with respect to a basis $\{e_i\}$ is the same as that of $\rho(gdg^{-1})$ with respect to a basis $\{ge_i\}$. As $d \to gdg^{-1}$ maps $D_{\underline{q}/\underline{p}}$ to $D_{\underline{q}'/\underline{p}}$, $I_{\underline{q}/\underline{p}}$ to $I_{\underline{q}'/\underline{p}}$ and $\mathrm{Frob}_{\underline{q}/\underline{p}}$ to $\mathrm{Frob}_{\underline{q}'/\underline{p}}$ the result follows. □

Remark. If $\dim \rho = 1$ then

$$P_{\underline{p}}(\rho, t) = \begin{cases} 1 - \rho(\mathrm{Frob}_{\underline{p}})t & \text{if } \rho^I = \rho \\ 1 & \text{if } \rho^{\mathrm{I}} = 0 \end{cases}$$

In general it is essentially the characteristic polynomials of $\mathrm{Frob}_{\underline{p}}$ on $\rho^{I_{\underline{p}}}$: If $P_{\underline{p}}(\rho, t) = 1 + a_1 t + a_{"} t^2 + \cdots + a_n t^n$ then characteristic polynomials is $t^n + a_1 t^{n-1} + \cdots + a_n$.

Remark. The polynomial $P_{\underline{p}}(\rho, T)$ has the form $1 - (aT + bT^2 + \dots)$ so (ignoring convergence questions)

$$\begin{aligned} \frac{1}{P_{\underline{p}}(\rho, T)} &= 1 + (aT + bT^2 + \dots) + (aT + bT^2 + \dots)^2 + \dots \\ &= 1 + a_p T + a_{p^2} T + \dots \end{aligned}$$

for some $a_{\underline{p}^i} \in \mathbb{C}$. Formally substituting this to the Euler product gives the *Artin L-series* for ρ.

$$\begin{aligned} L(\rho, s) &= \prod_{\underline{p}} (1 + a_{\underline{p}} N(\underline{p})^{-s} + a_{\underline{p}^s} N(\underline{p})^{-2s} + \dots) \\ &= \sum_{\underline{n} \text{ non-zero ideal of } K} a_{\underline{n}} N(\underline{n})^{-s} \end{aligned}$$

for some $a_{\underline{n}} \in \mathbb{C}$. Note that grouping ideals of equal norm yields an expression for $L(\rho, s)$ as an ordinary Dirichlet series.

Lemma 3.14. *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 $\prod_{\underline{p} \text{ prime of } K} (1 + a_{\underline{p}} N(\underline{p})^{-s} + \dots)$ (as in the previous remark) converges absolutely on $\mathrm{Re}(s) > 1$. This justifies rearrangement of the terms, and the expression as an ordinary Dirichlet series for $L(\rho, s)$ then proves analytically (Proposition 3.3). The polynomial $P_{\underline{p}}(\rho, T)$ factors over $\mathbb{C}$ as $P_{\underline{p}}(\rho, T) = (1 - \lambda_1 T)(1 - \lambda_2 T) \dots (1 - \lambda_k T)$ for some $k \leq \dim \rho$ with all $|\lambda_i| = 1$. So the coefficients of

$$\begin{aligned} \frac{1}{P_{\underline{p}}(\rho, T)} &= \frac{1}{\prod (1 - \lambda_i T)} \\ &= 1 + a_{\underline{p}} T + a_{\underline{p}^2} T^2 + \dots \end{aligned}$$

are bounded in absolute value by those of

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

Hence

$$\begin{aligned} \prod_{\underline{p}} \sum_n \left| a_{\underline{p}^n} \right| |N(\underline{p})^{-s}| &\leq \prod_{\underline{p}} \frac{1}{(1 - |N(\underline{p})^{-s}|)^{\dim \rho}} \\ &\leq \prod_{\underline{p}} \left(\frac{1}{1 - |p^{-s}|} \right)^{\dim \rho} (\underline{p} \text{above}\, p) \\ &= \zeta(\sigma)^{\dim_\rho [K:\mathbb{Q}]} \end{aligned}$$

where $\sigma = \mathrm{Re}(s)$. □

Proposition 3.15. *Let F/K be a Galois extension of number fields ρ a* $\mathrm{Gal}(F/K)$ *representation.*

1. *If ρ' is another* $\mathrm{Gal}(F/K)$*-representation then* $L(\rho \oplus \rho', s) = L(\rho, s)L(\rho', s)$
2. *If $N \lhd \mathrm{Gal}(F/K)$ lies in $\ker(\rho)$ so that ρ comes from a representation ρ'' of $\mathrm{Gal}(F^N/K) = G/N$ then $L(F/K, \rho, s) = L(F^N/K, \rho'', s)$.*
3. *(*Artin Formalisation*) If $\rho = \mathrm{Ind}_H^G \rho'''$ for a representation of $H \leq G$ then $L(F/K, \rho, s) = L(F/F^H, \rho''', s)$*

Proof. It suffices to check the statement prime-by-prime for the local polynomials

1. Clear (Note $(\rho \oplus \rho')^{I_p} = \rho^{I_p} \oplus \rho'^{I_p}$)
2. Straight from the definitions using: if $G = \mathrm{Gal}(F/K)$, $N \lhd G$, $\underline{q}$ a prime above $\underline{s}$ in F^N, above $\underline{p}$ is K. Then $D_{\underline{s}/\underline{p}} = D_{\underline{q}/\underline{p}}N/N$, $I_{\underline{s}/\underline{p}} = I_{\underline{q}/\underline{p}}N/N$, $\mathrm{Frob}_{\underline{q}/\underline{p}}N = \mathrm{Frob}_s/\underline{p}$ (proof, exercise)
3. This follows from Proposition 2.16: the second formula there show that the number of times $(1 - \zeta T)$ in $P_{\underline{p}}(\rho, T)$ and in $\prod_{\Sigma \text{ above } \underline{p}} P_{\underline{s}}(p''', T^{\underline{p}_{\Sigma_i/\underline{p}}})$ is the same.

□

Example. Let $K = \mathbb{Q}$, $F = \mathbb{Q}(\zeta_N)$. $G = \mathrm{Gal}(F/K) \cong (\mathbb{Z}/N\mathbb{Z})^*$. Then

$$\begin{aligned} \zeta_F(s) &= L(F/F, \mathbb{I}, s) \\ &= L(F/\mathbb{Q}, \mathrm{Ind}\mathbb{I}, s) \\ &= \prod_{\chi \in \widehat{G}} L(\chi, s) \end{aligned}$$

where $\widehat{G}$ is the set of irreducible representations of G. For general $F/\mathbb{Q}$ would have

$$\zeta_F(s) = \prod_{\rho \in \widehat{G}} L(\rho, s)^{\dim \rho}$$

3.4 Artin L-series for 1-dimesnional representation

Lemma 3.16. *Let $F = \mathbb{Q}(\zeta_N)$ and $\chi : \mathrm{Gal}(F/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$. Then*

$$L(F/\mathbb{Q}, \chi, s) = L_N(\chi, s) \cdot \prod_{p|N} \frac{1}{P_p(\chi, q^{-1})}$$

Proof. We can compare the Euler factor prime by prime. For $p|N$ we have equality as the one for $L_N(\chi, s)$ is 1 ($\chi(p) = 0$).

For $p \nmid N$, p is unramified in $\mathbb{Q}(\zeta_N)$ so $I_p = \{\mathrm{id}\}$ (so $\chi^{I_p} = \chi$) and $\mathrm{Frob}_p(\zeta_N) = \zeta_N^p \leftrightarrow p \mod (\mathbb{Z}/N\mathbb{Z})^*$. Thus

$$\begin{aligned} P_p(\chi, T) &= \det(1 - \mathrm{Frob}_p T | \chi^{I_p}) \\ &= 1 - \chi(\mathrm{Frob}_p)T \\ &= 1 - \chi(p)T \end{aligned}$$

as required □

Remark. When N is minimal, the last term is 1 and $L(\chi, s) = L_N(\chi, s)$.

Remark. By the Kroneckar-Weber theorem, every abelian extension of $\mathbb{Q}$ lies inside $\mathbb{Q}(\zeta_N)$ for some N. So if $\rho : \mathrm{Gal}(F/\mathbb{Q}) \to \mathbb{C}^*$ is a 1-dimensional representation then by Proposition 3.15 2. $L(\rho, s) = L(\rho'', s)$ for some $\rho'' : \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \to \mathbb{C}^*$ which is then essentially a Dirichlet L-function.

Theorem 3.17. (Hecke (1920)+ some Class Field Theory) *Let F/K be a Galois extension of number fields and $\psi : \mathrm{Gal}(F/K) \to \mathbb{C}^*$ a 1-dimensional representation. Then $L(\psi, s)$ has an analytic continuation to $\mathbb{C}$, except for a simple pole at $s = 1$ when $\psi = \mathbb{I}$.*

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

Proof. Way beyond the scope of this course □

Corollary 3.18. *If $\psi \neq \mathbb{I}$ then $L(\psi, 1) \neq 0$.*

Proof. By Proposition 3.15 2. we may assume F/K is abelian. Then by Proposition 3.15 1. and 3.

$$\begin{aligned} \zeta_F(s) &= L(F/K, \mathrm{Ind}\mathbb{I}, s) \\ &= \prod_{\chi \in \widehat{G}} L(F/K, \chi, s) \\ &= \zeta_K(s) \prod_{\chi \neq \mathbb{I}} L(F/K, \chi, s) \end{aligned}$$

As both ζ-functions have a simple pole and the rest are analytic, this implies $L(F/K, \chi, 1) \neq 0$. □