Algebraic Number Theory

Basics

- **Integral domain:** $rs = 0 \implies r = 0$ or $s = 0$.
- **Ideal:** A subset I of R such that
  - $(I, +)$ subgroup of $(R, +)$.
  - For any $r \in R$, $x \in I$, we have $rx \in I$.
- **Principal ideal:** Generated by on element $I = (x)$. i.e. $I = \{rx : r \in R\}$.
- **Quotient:** Let I be ideal of R. The quotient ring R/I is $\{r + I : r \in R\}$, where $r_1 + I = r_2 + I$ iff $r_1 - r_2 \in I$. Zero element is I and multiplicative identty is $1 + I$.
- **Maximal:** an ideal $I \neq R$ such that, if $I \subseteq J \subseteq R$, then $I = J$ or $J = R$ (i.e. no ideals bigger than I)
- **Prime:** An ideal $I \neq R$ s.t. $ab \in I \implies a \in I$ or $b \in I$
- Let I be an ideal of R
  - I is a prime ideal if and only if R/I is an integral domain.
  - I is a maximal ideal if and only if R/I is a field.

  Corollary: Every maximal ideal is prime

Galois Theory

- **Degree:** L/K has degree $[L : K] = \dim_K(L)$.
- **Tower law:** $[M : K] = [M : L][L : K]$
- **Automorphism group:** $\mathrm{Aut}(L/K) := \{\sigma : L \to L : \sigma$ field automorphism s.t. $\sigma|_K = \mathrm{Id}_K\}$

  Examples:
  - $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2$ (the identity, and $\sqrt{2} \mapsto -\sqrt{2}$)
  - $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}\}$
- **Galois extension:** For L/K finite, TFAE
  - $L^{\mathrm{Aut}(L/K)} := \{x \in L : \sigma(x) = x \ \forall \sigma \in \mathrm{Aut}(L/K)\} = K$
  - $\#\mathrm{Aut}(L/K) = [L : K]$
  - L/K is **normal** ($\forall \alpha \in L$, the min poly of α has roots in L) and **separable** ($\forall \alpha \in L$, the min poly of α has distinct roots in $\bar{K}$)
  - L/K is the splitting field of a separable polynomial $f \in K[T]$

- **Main Theorem:** Let L/K be Galois, then we have order-reversing mutually inverse bijections

$$\begin{aligned}\{\text{subextensions} K \subseteq M \subseteq L\} &\longrightarrow \{\text{ subgroups } H \leq \mathrm{Gal}(L/K)\} \\ M &\longmapsto \mathrm{Gal}(L/M) \\ \{x \in L : \sigma(x) = x\ \forall \sigma \in H\} &\longleftarrow H\end{aligned}$$

- **Finite fields:** If K finite field, then $K \cong \mathbb{F}_q$ where $q = p^r$ prime power. Moreover $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \iff n|m$
- $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois (is the splitting field of $X^q - X$) and $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is cyclic, generated by the **Frobenius**, denoted $\mathrm{Frob}_q : x \mapsto x^q$.

Number Fields

- **Number field:** A finite extension of $\mathbb{Q}$ (e.g. $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt[3]{2})$.
- **Ring of integers:** Let L be number field. THe ring of integers θ_L is the integral closure of $\mathbb{Z}$ in L.

$$\theta_L = \{\alpha \in L : \exists f \in \mathbb{Z}[T] \text{ monic s.t.} f(\alpha) = 0\}$$

  - θ is Dedekind domain.
  - All ideals have unique factorisation into prime ideals.

- **Class group:** We define the class group of θ_L as:

$$\mathrm{Cl}(\theta_L) = \{\text{ non-zero ideals } I \trianglelefteq \theta_L\}/\sim$$

  where ideals $A \sim B$ if there exists $x, y \in \theta_L$ s.t. $(x)I = (y)J$

- **Class number:** $h_L = \#\mathrm{Cl}(\theta_L)$
  - $\mathrm{Cl}(\theta_L)$ is a **finite** abelian group.
  - $h_L = 1$ if and only if θ_L is a princiapl ideal domain.
  - I.e. If θ_L Dededekind domain, then $h_L = 1$ iff θ_L is unique factorisation domain.

Lectures

1. Dedekind domains

- **Principal ideal domain:** An integral domain in which every ideal is principal (i.e. generated by a single element)
- **Discrete Valuation Ring**: A ring A which is
  - A principal ideal domain
  - Has a **unique** non-zero prime ideal m_A

  Note: m_a is maximal ideal ,and A is local ring.

  Fact: Every non-zero $x \in A$ can be expressed *uniquely* as $x = \alpha\pi^k$ where α is unit, π is uniformizer, and $k \in \mathbb{Z}_{\geq 0}$.
- **Uniformizer:** A generator π of the unique maximal ideal in a DVR is called a **uniformizer**.
- **Local ring**: Has a unique maximal ideal
- **Nakayama's lemma:** Let R be local ring, $P \subset R$ the unique maximal ideal, M a fin. gen. R-module. THen
  - If $M = PM$, then $M = 0$ (i.e. $M/PM = 0 \implies M = 0$)
  - If $N \leq M$ is an R-submodule s.t. $N + PM = M$, then $N = M$
- **Valuation:** Let K be a field. A **valuation** is a function $\nu : K^\times \to \mathbb{Z}$ such that
  - ν is surjective homomorphism
  - $\nu(x + y) \geq \min(\nu(x), \nu(y))$ for all $x, y, \in K^\times$ with **equality** if $\nu(x) \neq \nu(y)$.

  Examples:
  - Let $K = \mathbb{Q}$. We can define a valuation $\nu : \mathbb{Q}^\times \to \mathbb{Z}$ defined by $\nu(p^n \frac{r}{s})$ if $r, s \in \mathbb{Z}$ and p coprime to r and s.
  - Let K be the field of meromorphic functions on $\mathbb{C}$. Can define $\nu : K^\times \to \mathbb{Z}$ by $\nu(f) = \mathrm{ord}_{z=0} f(z)$.
- **Valuation of DVR:** Let A be a DVR with uniformiser π, and let $K = \mathrm{Frac}(A)$. Then can define a **valuation** $\nu(x) = n$, where $x = \pi^n u$ for some $n \in \mathbb{Z}$ and $u \in A^\times$.
- For any field K, there is a bijection between the valuations $\nu : K^\times \to \mathbb{Z}$ and the subrings $A \subset K$ s.t. A is a DVR and $\mathrm{Frac} A = K$.
- **Noetherian ring**: A ring where, if $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ is an ascending chain of ideals, then there exists N such that $I_N = I_{N+1} = \ldots$. Equivalently, a ring where every ideal is finitely generated (i.e there exist $a_1, \ldots, a_n \in I$ s.t. $I = Ra_1 + \ldots Ra_n$)
- **Integrally closed:** Let A, B be rings where $A \subseteq B$. B is integrally closed over A if, for all $b \in B$, there exist $a_1, \ldots, a_n \in A$ such that

  $$b^n + a_1 b^{n-1} + \ldots a_n = 0$$

  (i.e. b root of monic polnomial in A)

- **Integrally closed domain:** An integral domain R such that integral closure of R over $\text{Frac}(R)$ is itself.
- Let A be a Noetherian domain. Then TFAE:
  - A is a DVR
  - A is integrally closed in $K = \text{Frac}A$ and A has a unique non-zero prime ideal.
- **Mutiplicative subset:** A subset $S \subseteq A$ s.t. $1 \in S$ and $\forall x, y \in S, xy \in S$.
- **Fraction ring:** Let $S \subseteq A$ be multiplicative subset. Define $S^{-1}A$ as $A \times S/\sim$ where $(a, s) \sim (a', s')$ if there exists $t \in S$ s.t. $t(s'a - sa') = 0$. Notation: $\frac{a}{s} \in S^{-1}A$.
  - Zero element is $\frac{0}{1}$. Multiplicative identty is $\frac{1}{1}$.
  - Adddition: $\frac{a}{s} + \frac{a'}{s'} = \frac{as'+a's}{ss'}$
  - Multiplication: $\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$

  (*Note:* If $0 \in S$, then $S^{-1}A$ is just the trivial zero ring.)

  The map $A \to S^{-1}A$ given by $a \mapsto \frac{a}{1}$ is **ring homomorphism** with kernel $\{a \in A : \exists s \in S, sa = 0\}$
- **Fraction ring for modules:** Let $S \subseteq A$ be multiplicative subset. Let M be A-module. Define $S^{-1}M$ to be $M \times S/\sim$ where $(m, s) \sim (m', s')$ if there exists $t \in S$ s.t. $t(ms' - m's) = 0$.

  $S^{-1}M$ is a $S^{-1}A$-**module** via
  - Additive identity: $\frac{0}{1}$
  - Multiplication: $\frac{a}{s} \cdot \frac{m}{s'} = \frac{am}{ss'}$
  - Addition: $\frac{m}{s} + \frac{m'}{s'} = \frac{ms'+m's}{ss'}$
- If $f : M \to N$ is an A-module homomorphism, then there is a homomoprhism $S^{-1}f : S^{-1}M \to S^{-1}N$ given by $\frac{m}{s} \mapsto \frac{f(m)}{s}$.
- S^{-1} **functor:** Given the homoprhisms $f : M' \to M$ and $f' : M \to M''$, then $S^{-1}(f' \circ f) = S^{-1}f' \circ S^{-1}f$ (i.e. S^{-1} is a functor in the category of A-modules)
- **Exactness:** Let $M' \to M \to M''$ be an exact sequence of A-modules. Then $S^{-1}M' \to S^{-1}M \to S^{-1}M''$ is also exact.
  - If f is **surjective**, then so is $S^{-1}f$.
  - If f' is **injective** then so is $S^{-1}f'$
- **Ideal of fraction ring:** Let A be a ring with ideal $I \lhd A$. Since $I \to A$ is injective homorphism of A-modules, we have $S^{-1}I \to S^{-1}A$ injective homomorphism of A-modules. Therefore, $S^{-1}I$ is an **ideal** of $S^{-1}A$, which is the ideal:

$$S^{-1}I = \{\frac{x}{s} : x \in I \ s \in S\}$$

- There is a bijection:

$$\left\{\begin{array}{l}\text{prime ideals } P \subset A \\ \text{such that } P \cap S = \emptyset\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{prime ideals} \\ Q \subset S^{-1}A\end{array}\right\}$$

$$P \longmapsto S^{-1}P$$
$$f^{-1}(Q) \longleftarrow\!\shortmid\; Q$$

  where $f : A \to S^{-1}A$ is the natural ring homomorphism $a \mapsto \frac{a}{1}$

- Let A be a ring, with prime ideal $P \lhd A$. Then $S = A - P$ is a mulitplicative subset of A, and $S^{-1}A$ is a *local ring* with unique maximal ideal $S^{-1}P$.

  Notation: We write $A_p = (A - P)^{-1}A$

- **Dedekind domain:** A ring R where
  - R is Noetherian domain.
  - R is integrally closed (domain).
  - R has (Krull) dimension 1 (i.e. every nonzero prime ideal is maximal).

- Let A be a ring. TFAE:
  - A is a Dedekind domain.
  - A is Noetherian domain, and for every non-zero prime ideal $P \subset A$, the localisation A_p is a DVR.

- **Fractional ideal:** Let A be domain, $K = \text{Frac}(A)$. A **fractional ideal** of A is a finitely generated A-submodule of K.

  Equivalently, a fractional ideal I of A is an A-submodule of K, such that there exists $r \in A$ such that $rI \subset A$ (element which 'clears out denominators')

  Examples:
  - If $A = \mathbb{Z}$, then all ideals are principal (i.e. of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$). All fractional ideals are of the form $\frac{n}{m}\mathbb{Z}$ for some $n, m \in \mathbb{Z}$

  If $I, J \subset K$ are freactional ideals, then
  - $I + J = \{x + y : x \in I, y \in J\}$ is also fractional ideal.
  - $IJ = (xy : x \in I, y \in J)$ is also fractional ideal.
  - $(I : J) = \{x \in K : xJ \subset I\}$ is A-submodule of K (If J non-zero, then is also fractional ideal)

- Let A be a Noetherian domain, and $S \subset A$ a multiplicative subset. Then
  - IF I, J fractional ideals, then $S^{-1}I$ is a fractional ideal of $S^{-1}A$ and:
    * $S^{-1}(I + J) = S^{-1}I + S^{-1}J$
    * $S^{-1}(IJ) = S^{-1}I \cdot S^{-1}J$
  - If I, J are fractional ideals, and J is non-zero, then $(I : J)$ is a fractional ideal of A and $S^{-1}(I : J) = (S^{-1}I : S^{-1}J)$.

- Let A Dedekind domain. Let Div$A$ be set of non-zero fractional ideals. Div$A$ forms a **group** under the operation of multiplication of fractional ideals. (Inverse of I is $(A : I)$)

- **Valuation for fractional ideals:** Let A be Dedekind domain, let $P \subset A$ be prime ideal, and let $\nu_p : K^\times \to \mathbb{Z}$ be the valuation corresponding to A_p.

  THen for any $I \in \mathrm{Div}A$, we have $IA_p = (x)$ for some $x \in K^\times$. We define the **valuation of** I as the surjective homorphism $\nu_p(I) := \nu_p(x)$.

- Let A be Dedekind domain. Then for non-zero ideal $I \subset A$, there are only finitely many non-zero prime ideals $P \subset A$ such that $I \subset P$ (i.e. finitely many primes lying above I).

  Also, for any $I \in \mathrm{Div}A$, there are only finitely many non-zero priem ideals P such that $v_p(I)$ is finite.

- The map $\mathrm{Div}A \longrightarrow \oplus_p \mathbb{Z}$ is an **isomorphism**.

- For any $I \in \mathrm{Div}A$, we have $I = \prod_p p^{\nu_p(I)}$

- **Unique factorisation of ideals:** Let A be a Dedekind domain, and let $I \subset A$ be a non-zero ideal. Then I admits a unique expression:

  $$I = \prod_{i=1}^{n} P_i^{a_i}$$

  where the P_i are distinct prime ideals of A. This expression is *uniquely* determined upto re-ordering of terms.

Fact: For every number field, the ring of integers is always a Dedekind domain! (but not necessarily a PID)

2. Complete DVRs

- **Inverse System:** Given groups $A_i (i \in \mathbb{N})$ and homomorphisms $f_i : A_{i+1} \to A_i$ $(i \in \mathbb{N})$

$$A_1 \xleftarrow{f_1} A_2 \xleftarrow{f_2} A_3 \xleftarrow{f_3} A_4 \xleftarrow{f_4} \dots$$

- **Inverse limit:**

$$\varprojlim_i A_i = \left\{ (a_i) \in \prod_{i=1}^{\infty} A_i : \forall i \geq 1, f_i(a_{i+1}) = a_i \right\} \leq \prod_{i=1}^{\infty} A_i$$

  Fact: Inverse limit of groups/abelian groups/rings is a group/abelian group/ring.

- **Completion of DVR:** Let A be a DVR, with uniformiser π. Then we can consider the inverse system:

$$A/(\pi) \longleftarrow A/(\pi^2) \longleftarrow A/(\pi^3) \longleftarrow A/(\pi^4) \longleftarrow \dots$$

  with maps the natural quotient maps. We define the inverse limit to be $\hat{A} := \varprojlim_i A/(\pi^i)$.

  There is a natural homomorphism $A \longrightarrow \varprojlim_i A/(\pi^i)$.

- **Complete:** We say A is **complete** if $A \to \varprojlim_i A/(\pi^i)$ is an *isomorphism.* (A complete $\iff$ map is surjective)

  Note: The kernel of above map is $\bigcap_{i \geq 1} (\pi^i) = 0$. Therefore map is always an injective homomorphism.

- Let A be DVR with fraction field K and valuation $\nu : K^\times \to \mathbb{Z}$. Then TFAE:
  - A is complete.
  - A is complete as metric space w.r.t the metric

$$d(x, y) = \begin{cases} 0 & \text{if } x = y \\ 2^{-\nu(x-y)} & \text{if } x \neq y \end{cases}$$

  - K is complete as metric space w.r.t. metric given above

- **Ultrametric:** A metric d satisfying $d(x, z) \leq \max(d(x, y), d(y, z))$

  Useful facts:
  - Sequences (x_i) s.t. $|x_{n+1} - x_n| \to 0$ as $n \to \infty$ are Cauchy
  - All open balls (with positive radius) are closed, and all closed balls are open.

- **Totally disconnected:** A topological space is totally disconnected if the only connected subsets are the singletons (i.e. no non-trivial connected subsets)

- Let A be a DVR, with $\pi \in A$ a uniformizer. THen:
  - THe map $A \to \hat{A}$ is **injective**. $\hat{A}$ is a complete DVR, and π is a uniformizer of $\hat{A}$.
  - FOr all $i \geq 1$, the map $A/\pi^i A \to \hat{A}/\pi^i \hat{A}$ is an isomorphism.

- Let $X \subset A$ be a subset of representatives for the residue classes of $A/(\pi)$ with $0 \in X$. Then for all $a \in \hat{A}$, there exists a unique expression of the form

$$a = \sum_{i=0}^{\infty} a_i \pi^i$$

with $a_i \in X$ for all $i \geq 0$.

- **p-adic numbers:** Let p be a prime. We define the p **adic integers** $\mathbb{Z}_p = \hat{\mathbb{Z}}_{(p)}$ where $\mathbb{Z}_{(p)} = (\mathbb{Z} - (p))^{-1}\mathbb{Z}$ and the **p-adic rationals** $\mathbb{Q}_p = \operatorname{Frac} \mathbb{Z}_p$

  Fact: $p \in \mathbb{Z}_p$ is a uniformizer and the residue field $\mathbb{Z}_p/(p) \cong \mathbb{Z}/p\mathbb{Z}$

  Each element of $\mathbb{Z}_p$ has a unique expression: $\sum_{i=0}^{\infty} a_i p^i$, where $a_i \in \{0, 1, \ldots, p-1\}$

  Each element of $\mathbb{Q}_p$ has a unique expression: $\sum_{i \in \mathbb{Z}} a_i p^i$, where $a_i \in \{0, 1, \ldots, p-1\}$ with the set $\{i < 0 : a_i \neq 0\}$ finite.

  Multiplication and addition is done in the same way as for formal power series, except we now need to 'carry' digits

- **Hensel's lemma:** Let A be complete DVR. Let $f(x) \in A[x]$ be monic polynomial. Suppose there exists $\alpha \in A$ such that $v(f(\alpha)) > 2v(f'(\alpha))$. Then, there exists unique $a \in A$ such that $f(a) = 0$ and $v(a - \alpha) > v(f'(\alpha))$.

  Construction: Define a sequence of numners $a_1, a_2, \ldots$, where $a_1 = \alpha$ and

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$$

  Then $(a_n)_{n \geq 1}$ is a Cauchy seuqnece, and thus we have the limit $a := \lim_{n \to \infty} a_n$.

- **Hensel's corollary:** Let A complete DVR. Let $f(x) \in A[x]$ be monic, Let $k = A/(\pi)$ and $\bar{f}(x) = f(x) \bmod (\pi) \in k[x]$. Suppose there exists $\bar{\alpha} \in K$ a simle root of $\bar{f}(X)$. Then, there exists a unique $a \in A$ s.t. $f(a) = 0$ and $a \equiv \bar{\alpha} \bmod (\pi)$

  (this is specific case where $v(f'(\alpha)) = 0$)

- Squares in $\mathbb{Z}_p^\times$:
  - If p is odd, then $u \in \mathbb{Z}_p^\times$ is a square if and only if $u \bmod p \in \mathbb{F}_p^\times$ is a square.
  - If $p = 2$, then $u \in \mathbb{Z}_p^\times$ is a square if and only if $u \equiv 1 \bmod 8$. (i.e. if $u \bmod 8$ is a square in $(\mathbb{Z}/8\mathbb{Z})^\times$.

- Cubes in $\mathbb{Z}_p^\times$:
  - If $p \neq 3$, then $u \in \mathbb{Z}_p^\times$ is a cube if and only if $u \bmod p \in \mathbb{F}_p^\times$ is a cube.
  - If $p = 3$, then $u \in \mathbb{Z}_p^\times$ is a cube if and only if if $u \bmod 9$ is a cube in $(\mathbb{Z}/9\mathbb{Z})^\times$.

- n-th powers in $\mathbb{Z}_p^\times$:
  - If $p \not| n$, then $u \in \mathbb{Z}_p^\times$ is an n-th power if and only if $u \bmod p \in \mathbb{F}_p^\times$ is an n-th power.
  - If $p = n$, then then $u \in \mathbb{Z}_p^\times$ is an n-th power if and only if $u \bmod p^2 \in \mathbb{F}_{p^2}^\times$ is an n-th power.

- **Teichmuller lift:** There's a surjective homomorphism $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times$ given by $\sum_{i=0}^{\infty} a_i p^i \mapsto a_0 \bmod p$.

  There's exists a unique homomorphism $\tau : \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ s.t. for all $\bar{\alpha} \in \mathbb{F}_p^\times$, $\tau(\bar{\alpha}) \bmod p = \bar{\alpha}$. This is called the **Teichmuller lift**.

  (i.e. τ sends every $\bar{\alpha} \in \mathbb{F}_p^\times$ to the unique $(p-1)$-st root of unity in $\mathbb{Z}_p^\times$ that reduces to it, or in other words the unique root α of $X^p - X$ such that $\alpha \bmod p = \bar{\alpha}$)

  Examples:

  - $p = 2$, then $\tau(1) = 1$.
  - $p = 3$, then $\tau(1) = 1$, and

  $$\tau(2) = 2 + 2p + 2p^2 + 2p^3 + 2p^4 + 2p^5 + 2p^6 + 2p^7 + 2p^8 + 2p^9 + \cdots = -1$$

  - $p = 5$, then $\tau(1) = 1$, and

  $$\begin{aligned}
  \tau(2) &= 2 + 1p + 2p^2 + 1p^3 + 3p^4 + 4p^5 + 2p^6 + 3p^7 + 0p^8 + 3p^9 + \dots \\
  \tau(3) &= 3 + 3p + 2p^2 + 3p^3 + 1p^4 + 0p^5 + 2p^6 + 1p^7 + 4p^8 + 1p^9 + \dots \\
  \tau(4) &= 4 + 4p + 4p^2 + 4p^3 + 4p^4 + 4p^5 + 4p^6 + 4p^7 + 4p^8 + 4p^9 + \cdots = -1
  \end{aligned}$$

  - $p = 7$, then $\tau(1) = 1$, and

  $$\begin{aligned}
  \tau(2) &= 2 + 4p + 6p^2 + 3p^3 + 0p^4 + 2p^5 + 6p^6 + 2p^7 + 4p^8 + 3p^9 + \dots \\
  \tau(3) &= 3 + 4p + 6p^2 + 3p^3 + 0p^4 + 2p^5 + 6p^6 + 2p^7 + 4p^8 + 3p^9 + \dots \\
  \tau(4) &= 4 + 2p + 0p^2 + 3p^3 + 6p^4 + 4p^5 + 0p^6 + 4p^7 + 2p^8 + 3p^9 + \dots \\
  \tau(5) &= 5 + 2p + 0p^2 + 3p^3 + 6p^4 + 4p^5 + 0p^6 + 4p^7 + 2p^8 + 3p^9 + \dots \\
  \tau(6) &= 6 + 6p + 6p^2 + 6p^3 + 6p^4 + 6p^5 + 6p^6 + 6p^7 + 6p^8 + 6p^9 + \cdots = -1
  \end{aligned}$$

- We have the following isomorphism:

  $$\begin{array}{ccc}
  \mathbb{Q}_p^\times & \cong & \mathbb{Z} \times (1 + p\mathbb{Z}_p) \times \mathbb{F}_p^\times \\
  p^n \cdot u \cdot \tau(\bar{\alpha}) & \longmapsto & (n,\ u,\ \bar{\alpha})
  \end{array}$$

- We also have the isomorphism:

  $$\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^n \ \cong\ \mathbb{Z}/n\mathbb{Z} \times \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^n$$

- Let q be a prime that divides $p - 1$. Then $\mathbb{Q}_p$ has exactly $q + 1$ isomorphism classes of Galois extensions of degree q.

  Corollary: Let p be an odd prime. Then $\mathbb{Q}_p$ has exactly 3 isomorphism classes of quadratic extensions.

  Let $n \in \{1, 2, \dots, p-1\}$ be a **quadratic nonresidue** mod p. Then the three distinct quadratic extension of $\mathbb{Q}_p$ can be given as $\mathbb{Q}_p(\sqrt{n})$, $\mathbb{Q}_p(\sqrt{p})$, $\mathbb{Q}_p(\sqrt{np})$

3. Extensions of Dedekind domains

- **Integral:** Let A be Dedekind domain, $K = \mathrm{Frac}(A)$. Let E/K be finite separable extension. We say $\gamma \in E$ is **integral** over A if $\exists n \geq 1$, $a_1, \ldots, a_n \in A$ s.t.

$$\gamma^n + a_1\gamma^{n-1} + \cdots + a_n = 0$$

- Let A be Dedekind domain, $K = \mathrm{Frac}(A)$ and E finite separable extension of K. The following are equivalent:
  - γ integral over A
  - $A[\gamma]$ is a finitely generated A-module
  - There exists a non-zero $A[\gamma]$-submodule $M \subseteq E$ which is a finitely generated A-module.

- **Integral closure:** The integral closure of A in E is the set B consisting of all elements in E which are integral over A.

  Example: Let $A = \mathbb{Z}$, then $\mathrm{Frac}(A) = \mathbb{Q}$.
  - If $E = \mathbb{Q}(\sqrt{2})$, then $B = \mathbb{Z}(\sqrt{2})$.
  - If $E = \mathbb{Q}(\sqrt{5})$, then $B = \mathbb{Z}(\frac{1+\sqrt{5}}{2})$.
  - Let ζ be any root of unity. If $E = \mathbb{Q}(\zeta)$, then $B = \mathbb{Z}(\zeta)$.

- B is a subring of E, and B is integrally closed in E.

- Let E/K be finite separable extension. Let $T : E \times E \to K$ be the symmetric bilinear form defined by $T(x, y) = \mathrm{tr}_{E/K}(xy)$. Then T is **non-degenerate**. (i.e. for all non-zero $x \in E$, there exists $y \in E$ such that $T(x, y) \neq 0$)

  Localisation fact: Let $S \subseteq A$ be multiplicative subset, with $0 \notin S$. Then $S^{-1}A$ is Dedekind domain with $\mathrm{Frac}(S^{-1}A) = K$. Integral closure $S^{-1}A$ in E is $S^{-1}B$.

- *Fact:* B is *finitely generated A-module* and B is *Dedekind domain*

- **Setup:** A is Dedekind domain with $K = \mathrm{Frac}(A)$. E is finite sepearable extesnion of A. B is integral closure of A in E. Q is some non-zero prime ideal in B. Then $P = A \cap Q$ is non-zero prime ideal. We say Q **lies above** P.

$$\begin{array}{ccccc} E & \text{——} & B & \text{——} & \{Q_i\} \\ | & & | & & | \\ K & \text{——} & A & \text{——} & P \end{array}$$

- Let $Q \subset B$ and $P \subset A$ be non-zero prime ideals. Then the following are equivalent:
  - Q lies above P. (i.e. $P = Q \cap A$)
  - $Q \supset PB$.
  - Q appears in the prime factorisation of PB (i.e. $v_Q(PB) > 0$ where $v_Q : E^\times \to \mathbb{Z}$ is the valuation corresponding to Q)

  Fact: B/Q and A/P are fields and $(B/Q)/(A/P)$ is a **finite** extension.

- If Q lies above P, we define
  - **Residue degree:** $f_{Q/P} := [B/Q : A/P] \geq 1$
  - **Ramification index:** $e_{Q/P} := v_Q(PB) \geq 1$, where $v_Q : E^\times \to \mathbb{Z}$ is valuation corresponding to Q.
- **Prime factorisation of ideals:** $PB = Q_1^{e_{Q_1/P}} \dots Q_r^{e_{Q_r/P}}$
- Let $P \subset A$ be a non-zero prime ideal. Then

$$\sum_{Q\,:\,v_Q(PB)>0} e_{Q/P} f_{Q/P} = [E : K]$$

  (the sum running over all primes ideals Q of B lying over P.)
- Let P be non-zero prime ideal of A, and let $Q_1, Q_2, \dots, Q_r$ be all the prime ideals of B lying above P.
  - **Unramified:** If for all $i = 1, 2, \dots, r$, we have B/Q_i a seprable extension, and $e_{Q_i/P} = 1$, then we say P is **unramified** in B.
  - **Splits completely:** If for all $i = 1, 2 \dots, r$, we have $e_i = f_i = 1$, then we say P **splits completely** in B. (i.e. $r = [E : K]$)
  - **Ramified:** If $e_i > 1$ for some $i = 1, \dots, r$, then we say P is **ramified** in B.
  - **Ramifies completely:** If $r = 1$ and $f_1 = 1$ (and thus $e_1 = [E : K]$), we say that P **ramifies completely** in B.
  - **Inert:** If $r = 1$ and $e_1 = 1$ (and thus $f_1 = [E : K]$), we say that P is **inert**.
- **Ring of integers:** If $E/\mathbb{Q}$ is a number field, then we denote $\mathcal{O}_E$ as the integral closure of $\mathbb{Z}$ in E, called the *ring of integers* of E.

  If $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ squarefree, then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{d}) \arrow[r, dash] \arrow[d, dash] & \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \arrow[r, dash] \arrow[d, dash] & \{Q_i\} \arrow[d, dash] \\
\mathbb{Q} \arrow[r, dash] & \mathbb{Z} \arrow[r, dash] & (p) \quad p \text{ prime}
\end{tikzcd}$$

  To factorise (p), we ...
- **Prime factorisation for $E = \mathbb{Q}(\sqrt{d})$:** For p odd, then:

$$p \begin{cases} \text{splits completely} & \text{if } \left(\frac{d}{p}\right) = 1 \\ \text{is unramified (and not split)} & \text{if } \left(\frac{d}{p}\right) = -1 \\ \text{is ramified} & \text{if } p | d \end{cases}$$

  where $\left(\frac{d}{p}\right)$ is the Legendre symbol which is 1 iff d is square mod p

(Euler's criterion states $\left(\frac{d}{p}\right) \equiv_p d^{(p-1)/2}$)

For $p = 2$:

$$2 \begin{cases} \text{splits completely} & \text{if } d \equiv 1 \pmod 4 \text{ and } \frac{1-d}{4} \text{ even} \quad (d \equiv_8 1) \\ \text{is unramified (and not split)} & \text{if } d \equiv 1 \pmod 4 \text{ and } \frac{1-d}{4} \text{ odd} \quad (d \equiv_8 5) \\ \text{is ramified} & \text{if } d \equiv 2, 3 \pmod 4 \end{cases}$$

- **Factorisation of pO_E for quadratic extensions:** If p is odd, then:

$$pO_E = \begin{cases} (pO_E + (..)O_E)(pO_E + (..)O_E) & \text{if } \left(\frac{d}{p}\right) = 1 \\ pO_E & \text{if } \left(\frac{d}{p}\right) = -1 \\ (pO_E + (..)O_E)^2 & \text{if } p \mid d \end{cases}$$

- Let A, K, E, B given in setup. Suppose E/K is Galois, and let $G = \mathrm{Gal}(E/k)$. Then for all $\sigma \in G$, $\sigma(B) = B$. (i.e. the action of G on E leaves B invariant)
- Let E/K be Galois, and let $Q \subset B$ be non-zero prime ideal, with $P = Q \cap A$. Then
  1. G acts *transitively* on prime ideals of B lying above P.
     (i.e. only one orbit. $\forall Q_1, Q_2 \supseteq P, \exists \sigma \in G$ s.t. $\sigma(Q_1) = Q_2$)
  2. For all $\sigma \in G$, $f_{\sigma(Q)/P} = f_{Q/P}$ and $e_{\sigma(Q)/P} = e_{Q/P}$.
     (i.e. e and f depend only on P, and not Q)
  3. Let $g_{Q/P}$ be the number of prime ideals lying above P. Then $e_{Q/P} f_{Q/P} g_{Q/P} = [E : K] = |G|$
- **Decomposition group:** Setup above, Q lies above P. The decomposition group $D_{Q/P} = \mathrm{Stab}_G(Q) = \{\sigma \in G : \sigma(Q) = Q\}$.
- Let E/K Galois. Suppose $Q \subset B$ lies above $P \subset A$, and suppose that $(B/Q)/(A/P)$ is separable. Then
  - $(B/Q)/(A/P)$ is a **Galois** field extension.
  - The map

$$\begin{aligned} D_{Q/P} &\longrightarrow \mathrm{Gal}((B/Q)/(A/P)) \\ \sigma &\longmapsto \sigma|_B \bmod Q \end{aligned}$$

    is a **surjective** group homomorphism.
- **Inertia group:** Define the inertia group at Q as $I_{Q/P} = \ker(D_{Q/P} \to \mathrm{Gal}(k_Q/k_P)) = \{$automorphisms of E/K that induce the identity on $B/Q\}$

  Fact: $|I_{Q/P}| = e_{Q/P}$, and thus $I_{Q/P}$ is trivial (and thus $D_{Q/P} \to \mathrm{Gal}(k_Q/k_P)$ an isomorphism) iff Q is unramified over P.
- **Frobenius automorphism at Q:** If P is unramified in E, then we have an element

$$\mathrm{Frob}_{Q/P} \in D_{Q/P} \subset G$$

  defined as the unique element in $D_{Q/P}$ which induces the Frobenius automorphism on the residue field extension k_Q/k_P.

- Let $f(X) = X^n + a_1X^{n-1} + a_2X^{n-2} + a_n \in \mathbb{Z}[X]$ be irreducible. Let E be the splitting field of $f(X)$ over $\mathbb{Q}$, and let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $f(X)$.

  (note that $\mathrm{Gal}(E/\mathbb{Q})$ can be identified as a subgroup of the symmetric group on $\alpha_1, \alpha_2, \ldots, \alpha_n$), i.e. we have

  $$\mathrm{Gal}(E/\mathbb{Q}) \hookrightarrow S_n = \mathrm{Sym}(\alpha_1, \alpha_2, \ldots \alpha_n)$$

  Now suppose p is a prime number such that $\bar{f}(X) = f(X) =$ mod $p \in \mathbb{F}_p[X]$ factors as

  $$\bar{f}(X) = \prod_{i=1}^{r} \bar{f}_i(X),$$

  where $\bar{f}_1(X), \bar{f}_2(X), \ldots, \bar{f}_r(X)$ are distinct monic irreducible polynomials in $\mathbb{F}_p[x]$.

  Then $\mathrm{Gal}(E/\mathbb{Q})$ contains a permutation of cycle type $(d_1)(d_2)\ldots(d_r)$ where $d_i = \deg \bar{f}_i(X)$ (i.e. there's a permutation which has a cycle of length d_1, a cycle of length d_2, ..., and a cycle of length d_r)

- **Passage to completion:** Let A be Dedekind domain, with $K = \mathrm{Frac}(A)$. Let E/K be finite separable extension, and B the integral closure of A in E. Let $P \subset A$ be a non-zero prime ideal, and let $Q \subset B$ be a prime ideal lying above P. Then we have

  1. There's a natural homomorphism $\hat{A}_P \to \hat{B}_Q$ extending the map $A \to B$.
  2. Let $K_p = \mathrm{Frac}\hat{A}_p$, and $E_Q = \mathrm{Frac}\hat{B}_Q$. Then E_Q/K_p is finite separable extension, $\hat{B}_Q$ is integral closure of $\hat{A}_P$ in E_Q and $E_Q = K_p \cdot E$.
  3. We have $e_{Q/P} = e_{Q\hat{B}_Q/P\hat{A}_P}$ and $f_{Q/P} = f_{Q\hat{B}_Q/P\hat{A}_p}$ and $[E_Q : K_P] = e_{Q/P}f_{Q/P}$.
  4. If E/K Galois, then E_Q/K_P also Galois, and there's a natural *isomorphism* $D_{Q/P} \to \mathrm{Gal}(E_Q/K_P)$

- **Bijection between prime ideals and irreducible factors:** Let A be Dedekind domain, with $K = \mathrm{Frac}(A)$. Let E/K be finite separable extension, and B the integral closure of A in E. Let $E = K(\alpha)$ and let $f(X) \in K[X]$ be minimal polynomial of α. Then there's a **bijection** for any non-zero prime ideal $P \subset A$:

  $$\left\{ \begin{array}{c} \text{Prime ideals } Q \subset B \\ \text{lying above } P \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Irreducible factors} \\ g(X) \text{ of } f(X) \text{ in } K_p[X] \end{array} \right\}$$

  $$Q \longmapsto \begin{array}{c} \text{Unique irreducible factor} \\ g(X) \text{ of } f(X) \text{ in } K_p[X] \\ \text{such that } g(\alpha) = 0 \text{ in } E_Q \end{array}$$

  Example: Let $A = \mathbb{Z}$, then $K = \mathbb{Q}$ and let $E = \mathbb{Q}(\sqrt{d})$, and then $B = O_E$. Let (p) be a prime in $\mathbb{Z}$. Thus, the prime ideals of pO_E are in bijection with irreducible factors of $X^2 - d$ in $\mathbb{Q}_p[X]$.

4. Extensions of complete DVRs

- **Complete discrete valuation field**. We call a pair (K, v_k) a CDVF if K is a field and $v_K : K^\times \to \mathbb{Z}$ is a valuation and the corresponding DVR $A_K = \{x \in K^\times : v_K(x) \geq 0\} \cup \{0\}$ is complete.

  Examples:

  - $K = \mathbb{Q}_p$ (completion of $\mathbb{Q}$ w.r.t v_p). Coresponding DVR is $\mathbb{Z}_p$, and residue field is $\mathbb{F}_p$.
  - $K((X))$ (formal power series over field K, completion of $K(X)$ w.r.t v_X) i.e. element of the form
  $$\sum_{n\in\mathbb{Z}} a_n X^n$$
  where $a_n \in K$ and $a_n = 0$ for all but finitely many negative n. Corresponding DVR is $K[[X]]$ (no negative terms) and residue field is K.

  Notation: Uniformizer is $\pi_K \in A_K$. Residue field is $k_K = A_K/(\pi_K)$.

- Let K be a CDVF, and let E/K be a finite separable extension, Then E has a natural structure of CDVF.

- **Extension of CDVFs:** An extension E/K such that K is a CDVF, E/K is finite separable extension, and E has the natural structure of CDVF, with the valuation v_E given by the above lemma.

  Setup:

  - A_E and A_K are DVRs.
  - **Residue degree:** $f_{E/K} := f_{(\pi_E)/(\pi_K)} = [k_E : k_K]$
  - **Ramification index:** $e_{E/K} := e_{(\pi_E)/(\pi_K)} = v_E(\pi_K)$
  - If v_E is restricted to $K^\times$, then we have $v_E|_{K^\times} = e_{E/K} v_K$
  - $[E : K] = e_{E/K} \cdot f_{E/K}$

- Let E/K be an extension of CDVFs. Then:

  - If E/K is Galois, then for all $\sigma \in \mathrm{Gal}(E/K)$, $x \in E$, $v_E(\sigma(x)) = v_E(x)$
  - In general (not assuming Galois), for all $x \in E^\times$, we have
  $$v_E(x) = \frac{1}{f_{E/K}} v_K(N_{E/K}(x))$$

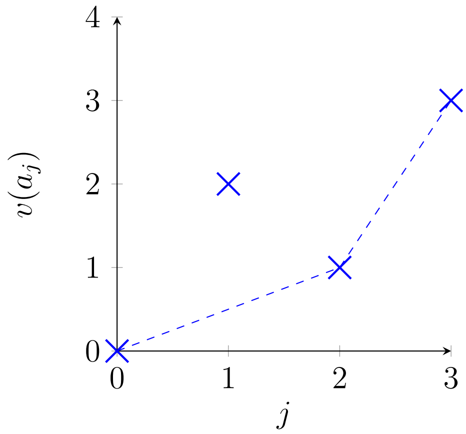
- **Newton polygon:** Let A be a DVR, $K = \mathrm{Frac}(A)$, and let
  $$f(X) = X^n + a_1 X^{n-1} + a_2 X^{n-2} \cdots + a_n$$
  be a polynomial in $K[X]$ with $a_n \neq 0$. Then the **Newton polygon** $N_K(f)$ is the graph of the largest piecewise linear continuous function $N : [0, n] \to \mathbb{R}$ s.t.

  - $N(0) = 0$ and $N(n) = v(a_n)$
  - For all $j = 1, 2, \ldots, n-1$, $N(j) \leq v(a_j)$ if $a_j \neq 0$.
  - N is convex (i.e. the sequence of slopes of line segments of $N_K(f)$ is increasing).

Equivalently, N is the lower convex hull of the points $(j, v(a_j))$, for $j = 0, 1, \ldots, n$.

- **Slopes:** The slopes of $N_k(f)$ are the slopes/derivatives of the line segments.
- **Multiplicity:** The multiplicity of a slope is the length of the projection of the corresponding line segment to the x-axis.

Example: Let $K = \mathbb{Q}_5$, and let $f(X) = X^3 + 25X^2 + 5X + 125$. Then the Newton polygon $N_{\mathbb{Q}_5}(f)$ looks like:



The slopes are $\frac{1}{2}$ (with multiplicity 2) and 2 (with multiplicity 1).

- Let A be DVR, $K = \mathrm{Frac}(A)$, and let $\alpha_1, \ldots, \alpha_n \in K^\times$ be such that $f(X)$ factors as

$$f(X) = \prod_{i=1}^{n}(X - \alpha_i) = X^n + a_1X^{n-1} + a_2X^{n-2} + \cdots + a_n \in K[x]$$

  Let $\lambda_i = v(\alpha_i)$, $i = 1, \ldots, n$. Then $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the slopes of $N_k(f)$ counted with multiplicity.

  In particular, the slopes of $N_K(f)$ are all integers.

- Let K be a CDVF, and let $f(X) \in K[x]$, $a_n \neq 0$ be separable. Let $\lambda_1 < \lambda_2 < \cdots < \lambda_r$, be the slopes of $N_K(f)$, where λ_i occurs with multiplicity $m_i \geq 1$.

  Then there exists a unique factorisation $f(X) = \prod_{i=1}^{r} g_i(X)$ in $K[x]$ where for all $i = 1, \ldots, r$, $g_i(X)$ is a monic polynomial with degree $\deg(g_i) = m_i$ and $N_K(g_i)$ has a single slope λ_i.

  (i.e. if $N_K(f)$ has r distinct slopes, then f can be factorised in to (at least) r factors)

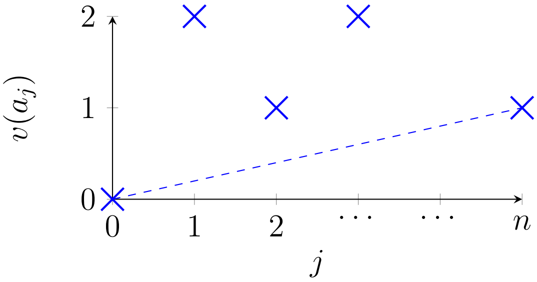
- Let E/K extension of CDVFs, then

  - E/K is **unramified** if k_E/k_K is separable and $e_{E/K} = 1$. (and thus $f_{E/K} = [E : K]$)
  - E/K is **totally unramified** if $f_{E/K} = 1$. (and thus $e_{E/K} = [E : K]$)

- **Eisenstein:** Let A be DVR, with $K = \mathrm{Frac}(A)$. We say $f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in A[X]$ is Eisenstein if $v_k(a_i) \geq 1$ for each $i = 1, \ldots, n-1$ such that $a_i \neq 0$, and $v_k(a_n) = 1$.

  Fact: For any monic $f(X) \in K[X]$, f is Eisenstein if and only if $N_K(f)$ is a single line segment of slope $\frac{1}{n}$.

  Example:



Constructing totally ramified extensions:

- Let E/K be totally ramified extension of CDVFs. Let $f(x) \in K[x]$ be the minimal polynomial of π_E. Then $f(X)$ is Eisenstein and $E = K(\pi_E)$.

- Let K be a CDVF, and let $f(X) \in K[X]$ be a separable polynomial which is Eisenstein. Then $f(X)$ is irreducible and if $E = K[x]/(f(X))$, then E/K is totally ramified and $X \bmod (f(X))$ is a uniformizer in A_E.

Constructing unramified extensions:

- Let K be a CDVF. Let ℓ/k_K be a finite separable extension. Then there exists an extension L/K of CDVFs and an isomorphism $i : \ell \to k_L$ with the following property: For any extension E/K of CDVFs and homomorphism $j : \ell \to k_E$ there exists a unique K-embedding $J : L \to E$ such that the diagram commutes:

$$\begin{tikzcd} & \ell \arrow[dr, "j"] & \\ k_L \arrow[ur, "i^{-1}"] \arrow[rr, "\exists!\ \bar{J}"'] & & k_E \end{tikzcd}$$

(i.e. $J : L \to E$ induces $j \circ i^{-1}$ on residue fields)

Moreover, L/K is **unramified**.

- Let p be a prime. Then for any $n \geq 1$, there is a *unique* unramified extension of $\mathbb{Q}_p$ of degree n (up to isomorphism).

Fact: For any $n \geq 1$, there is a unique extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ of degree n up to isomorphism.

- Let E/K be an extension of CDVFs, with k_E/k_K separable. Then there exists a unique subextension E_0/K which is unramified and such that $k_{E_0} = k_E$.

Then $f_{E_0/K} = f_{E/K}$ and $e_{E/E_0} = e_{E/K}$. Thus we have

$$E \xrightarrow{\text{totally ramified}} E_0 \xrightarrow{\text{unramified}} K$$

If E_1/K is any subextension which is unramified, then E_0 contains E_1. We therefore call E_0 the **maximal unramified subextension**.

- Let E/K be a Galois extension of CDVFs, with k_E/k_K separable. Then the maximal unramified subextension E_0 of E/K is $E^{I_{E/K}}$.

We always have a tower, with corresponding Galois groups:

$$\begin{tikzcd} E \arrow[r] \arrow[rr, bend left, no head, "G=\mathrm{Gal}(E/K)"] \arrow[r, bend right, no head, "I_{E/K}"'] & E_0 \arrow[r] \arrow[r, bend right, no head, "\mathrm{Gal}(k_E/k_K)"'] & K \end{tikzcd}$$

- **Lower ramification group:** Let $i \geq 0$. We define the ***i*-th lower ramification group** of $G = \mathrm{Gal}(E/K)$ to be

$$G_i := \ker(G \to \mathrm{Aut}(A_E/(\pi_E^{i+1}))$$
$$\text{or equivalently} \quad G_i = \{\sigma \in G : \text{for all } x \in A_E,\ \sigma(x) \equiv x \bmod (\pi_E^{i+1})\}$$

  By convention $G_{-1} = G$.

  - Informally, G_i is set of elements which fix the first $i+1$ digits of the π_E-adic expansion of elements of A_E.
  - $G_0 = \ker(G \to \mathrm{Aut}(A_E/(\pi_E)) = \ker(G \to \mathrm{Gal}(k_E/k_k) = I_{E/K}$ is the usual inertia group.
  - $G_{-1} \geq G_0 \geq G_1 \geq G_2 \geq G_3 \geq \dots$ and $\bigcap_{i \geq 0} G_i = \{1\}$.
  - Each G_i is normal subgroup in G. If $E/L/K$ is an intermediate extension and $H = \mathrm{Gal}(E/L)$, then $H_i = H \cap G_i$.

- Suppose $\sigma \in G_0$. Then for any $i \geq 0$, we have

$$\sigma \in G_i \iff v_E(\sigma(\pi_E) - \pi_E) \geq i + 1$$

  Examples:

  - Let E/K be $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$. E is splitting field of $X^2 - 2$ which is Eisenstein. So this is **totally ramified extension**, can take $\pi_E = \sqrt{2}$. Let $G = \{1, s\}$ Thus

$$G = G_0 = G_1 = G_2$$
$$\text{and} \quad \{1\} = G_3 = G_4 = G_5 = \dots$$

  - Let E/K be $\mathbb{Q}_2(\sqrt{3})/\mathbb{Q}_2$. E is splitting field of $X^2 - 3$. Can take $\pi_E = 1 + \sqrt{3}$ (min polynomial of π_E is $X^2 - 2X - 2$). Let $G = \{1, t\}$ Note $v_E(t(\pi_E) - \pi_E) = v_E(-2\sqrt{3}) = 2$. Thus

$$G = G_0 = G_1$$
$$\text{and} \quad \{1\} = G_2 = G_3 = G_4 = \dots$$

  - Let E/K be $\mathbb{Q}_2(i)/\mathbb{Q}_2$. E is splitting field of $X^2 + 1$. Can take $\pi_E = 1 + i$ (min polynomial of π_E is $X^2 - 2X + 2$). Let $G = \{1, t\}$. Thus

$$G = G_0 = G_1$$
$$\text{and} \quad \{1\} = G_2 = G_3 = G_4 = \dots.$$

  - Let E/K be $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$. E is splitting field of X^2-5. This is **unramified** extension. Can take $\pi_E = 2$. Let $G = \{1, t\}$. Thus

$$\{1\} = G_0 = G_1 = G_2 = G_3 = \dots.$$

- Let E/K be $\mathbb{Q}_2(\sqrt{2}, i)/\mathbb{Q}_2$. Can take $\pi_E = \zeta_8 - 1$. Let $G = \{1, s, t, st\}$. Thus

$$G = G_0 = G_1$$
$$\text{and} \quad \{1, s\} = G_2 = G_3$$
$$\text{and} \quad \{1\} = G_4 = G_5 = G_6 \dots$$

- Let $\pi \in A_E$ be a uniformizer, and let $s \in G_0$ and $i \geq 0$. Then

$$s \in G_i \iff s(\pi)/\pi \equiv 1 \bmod (\pi^i)$$

- Let E/K be a Galois extension of CDVFs, with k_E/k_K separable. Let $\pi \in A_E$ be a uniformizer. Then
  - There exists an injective homomorphism $G_0/G_1 \to k_E^\times$, given by the formula

    $$s \longmapsto s(\pi)/\pi \bmod \mathfrak{m}_L$$

    In particular, G_0/G_1 is cyclic of order prime to p if char $k_E = p > 0$.

    Note: Any finite subgroup of the multiplicative group of a field is cyclic of order prime to p if characteristic is $p > 0$.
  - If $i \geq 1$, then there's an injective homomorphism $G_i/G_{i+1} \to (k_E, +)$. In particular, G_i/G_{i+1} is **abelian** and

    $$G_i/G_{i+1} = \begin{cases} \text{trivial} & \text{if char } k_E = 0 \\ \mathbb{F}_p\text{-vector space} & \text{if char } k_E = p > 0 \end{cases}$$

  - The quotient G_0/G_1 is cyclic, and G_1 is:

    $$G_1 = \begin{cases} \text{trivial} & \text{if char } k_E = 0 \\ \text{the unique } p\text{-Sylow subgroup of } G_0 & \text{if char } k_E = p > 0 \end{cases}$$

- **Soluble group:** Let G be a group. G is **soluble** if there exist subgroups $G_0, G_1, G_2 \dots, G_k$ such that

  $$1 = G_0 < G_1 < G_2 < \cdots < G_k = G$$

  such that G_{j-1} is normal in G_j and such that G_j/G_{j-1} is an abelian group for all $j = 1, 2, \dots, k$. (i.e. G can be constructed from abelian groups using extensions)

  Examples: Any abelian group, any nilpotent group, any finite group of odd order (Feit-Thompson theorem), any finite group of order < 60

  Non-examples: The groups A_n and S_n for $n > 4$ are **not** soluble (indeed, A_5 is the smallest non-soluble group). Any non-cyclic simple group is not soluble.

  Orders of non-soluble groups: $60, 120, 168, 180, 240, 300, 336, 360, \dots$

- The group $I_{L/K} = G_0$ is **soluble**. If the residue field k_K is finite, then the group $\mathrm{Gal}(L/K)$ is soluble.

  Corollary: There is no Galois extension $E/\mathbb{Q}_p$ with Galois group A_5.

- **Tamely/Wildly ramified:** Let E/K be an extension of CDVFs. We say that the extension is **tamely ramified** if either $\mathrm{char}(k_E) = 0$ or $\mathrm{char}(k_E) = p > 0$ and $p \nmid e_{E/K}$.

  Otherwise, if $\mathrm{char}(k_E) = p$ and $p | e_{E/K}$, then we say E/K is **wildly ramified**.

  Note: If E/K is Galois and k_E/k_K is separable, then

  $$E/K \text{ is tamely ramified} \iff G_1 = \{1\}$$

- Let E/K be a Galois extension of CDVFs, which is both **totally** and **tamely** ramified (i.e. $e_{E/K} = [E : K]$ and if $\text{char} k_E = p > 0$, then $p \not| e_{E/K}$)

  Then if $n = [E : K]$, then K contains all the n n-th roots of unity and there exists a uniformiser $\pi_K \in A_K$ such that $E = K(\sqrt[n]{\pi_K})$.

  Constructing upper ramification groups:

- For any $u \in \mathbb{R}_{\geq 0}$, we define $G_u := G_{\lceil u \rceil}$. We now define the ramification function $\varphi_{E/K}(u)$ as
$$\varphi_{E/K}(u) = \int_{t=0}^{u} [G_0 : G_t]^{-1} dt$$
  Note: $\varphi_{E/K}(u)$ is continuous, strictly increasing, piecewise linear function, with discontinies of $\varphi'_{E/K}(u)$ occuring only at integer values. Thus $\varphi_{E/K} : [0, \infty) \to [0, \infty)$ is a *homeomorphism*.

- We now define $\psi_{E/K} = \varphi_{E/K}^{-1} : [0, \infty) \to [0, \infty)$ (inverse function of $\varphi_{E/K}$).

- **Upper ramification groups:** Let $v \in \mathbb{R}_{\geq 0}$. We define the v-th upper ramification group as
$$G^v := G_{\psi_{E/K}(v)}$$
  We say v is a **jump** in the upper ramification groups if $G^v \neq G^{v+\epsilon}$ for any $\epsilon > 0$.

  Note: The jumps in the lower ramification groups G_n must be integer values, but the jumps in the upper ramification groups G^v can occur at rational values.

  Example:

- Let E/K be a Galois extension of CDVFs, with k_E/k_K separable and $G = \text{Gal}(E/K)$. We define $i_G : G \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ by
$$i_G(s) = \begin{cases} \infty & \text{if } s = \{1\} \\ 1 + \sup\{i : s \in G_i\} & \text{if } s \neq \{1\} \end{cases}$$
  Therefore, we have
$$i_G(s) \geq i + 1 \iff s \in G_i$$

- For any $u \in \mathbb{R}_{\geq 0}$, we have
$$\varphi_{E/K}(u) + 1 = \frac{1}{|G_0|} \sum_{s \in G} \min(i_G(s), u + 1)$$

- Suppose there exists $\alpha \in A_E$ such that $A_E = A_K[\alpha]$. Then $i_G(s) = v_E(s(\alpha) - \alpha)$.

- THere exists $\alpha \in A_E$ such that $A_E = A_K[\alpha]$.

- Let H be a normal subgroup of G, and let $L = E^H$, so we have $\text{Gal}(L/K) = G/H$. Let $s \in G$. Then
$$i_{G/H}(sH) = \frac{1}{e_{E/L}} \sum_{t \in H} i_G(st)$$

- Let H be a normal subgroup of G, and let $L = E^H$. Define the function $j : G/H \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ by
$$j(sH) := \sup_{t \in H} i_G(st)$$
  Then we have
$$i_{G/H}(sH) = 1 + \varphi_{E/L}(j(sH) - 1)$$

- **Herbrand's theorem:** Let H be a normal subgroup of G, and let $L = E^H$. If $u \in \mathbb{R}_{\geq 0}$ and $v = \varphi_{E/L}(u)$, then:

$$(G/H)_v = G_u H/H \quad (= \mathrm{Im}(G_u \to G/H))$$

- Let H be a normal subgroup of G, and let $L = E^H$. We have that

$$\varphi_{E/K} = \varphi_{L/K} \circ \varphi_{E/L}$$

- Let H be a normal subgroup of G, and let $L = E^H$. For any $v \geq 0$, we have

$$(G/H)^v = G^v H/H$$

- Let E/K be an extension of CDVFs (not necessarily Galois), with k_E/k_K separable. If $v \in \mathbb{R}_{\geq 0}$, then we define

$$E^v := E \cap L^{G^v}$$

  where L/E is any extension of CDVFs with k_L/k_K seperable such that L/K is Galois and $G = \mathrm{Gal}(L/K)$.

  Note: E^v is an intermediate extension of E/K and is *independent* of the choice of L.

- Let E/K be an extension of CDVFs (not necessarily Galois), with k_E/k_K separable. We have
  - E^0 is the maximal unramified subextension.
  - If $v \leq v'$ then $E^v \subseteq E^{v'}$, and for sufficiently large v, $E^v = E$.
  - If $E/M/K$ is an intermediate extension, then $M^v = M \cap E^v$.
  - If E/M and N/K are two intermediate extensions, then $M^v \cdot N^v \subset (M \cdot N)^v$.
    In particular, if $M^v = M$ and $N^v = N$, then $(M \cdot N)^v = M \cdot N$.

- **Hasse-Arf Theorem:** Let $K/\mathbb{Q}_p$ be a finite extension, and let E/K be an abelain extension (i.e. E/K is a Galois extension and $\mathbf{Gal}(E/K)$ is abelian). Then all the jumps in the upper ramification groups are integers.

- **Conductor ideal:** Let $K/\mathbb{Q}_p$ be a finite extension, and let E/K be an abelian extension. We define the **conductor ideal** $C_{E/K}$ of A_K to be (π_K^a) where

$$a := \inf\{n \in \mathbb{Z}_{\geq 0} : G^n = \{1\}\} = 1 + \text{ highest jump}$$

  Note: $C_{E/K} = A_K$ the unit ideal $\iff$ E/K is unramified.

- Let $K/\mathbb{Q}_p$ be a finite extension, and let E/K be a Galois extension. Let $E_1, E_2/K$ be subextensions of E/K which are abelian over K. Then $E_1 \cdot E_2$ is abelian over K and

$$C_{E_1 \cdot E_2/K} = \mathrm{lcm}(C_{E_1/K}, C_{E_2/K}).$$

5. Global Class Field Theory

Fix a number field K. GCFT aims to describe all abelian extensions E/K.

- **Conductor ideal:** Let E/K be abelian extension of number fields. The conductor ideal is the unique ideal $C_{E/K} \subseteq \mathcal{O}_K$ s.t. for any non-zero prime ideal $P \subset \mathcal{O}_K$ and any prime ideal $Q \subseteq \mathcal{O}_E$ lying above P, we have $C_{E/K} A_{K_p} = C_{E_q/k_p}$.

  Equivalently, $v_p(C_{E/k}) = v_p(C_{E_q/k_p})$, and thus
$$C_{E/K} = \prod_{P \subset \mathcal{O}_K} P^{v_P(C_{E_Q/K_P})}$$

- Let E/K be extension of number fields. Thus for all but finitely many prime ideals $P \subset \mathcal{O}_K$, non-zero, P is unramified in $\mathcal{O}_E$.
  - If $K = \mathbb{Q}(\alpha)$ for $\alpha \in \mathcal{O}_K$ and $f(X) \in \mathbb{Z}[X]$ is the minimnal polynomial of α, then disc $\mathcal{O}_k \mid \mathrm{disc} f$.
  - If p prime, then $p | \mathrm{disc}\mathcal{O}_K$ if and only if p is ramified in $\mathcal{O}_K$ (i.e. $e_i > 1$ for some i).
  -

- **Kronecker-Weber theorem:** Let $L/\mathbb{Q}$ be an abelian extension. Then there exists $N \in \mathbb{Z}_{\geq 1}$ such that $L \subset \mathbb{Q}(\zeta_N)$. Moreover
$$L \subset \mathbb{Q}(\zeta_N) \iff C_{L/\mathbb{Q}} \mid (N)$$

- Let $N \geq 1$ be an integer, and let $\zeta_N = e^{2\pi i/N}$ be a primitive n-th root of unity. We have that the extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is **abelian**, and the isomorphism:
$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) &\longleftrightarrow (\mathbb{Z}/N\mathbb{Z})^\times \\ \begin{matrix} \sigma \text{ such that} \\ \sigma(\zeta_N) = \zeta_N^a \end{matrix} &\longmapsto a \pmod N \end{aligned}$$

  We have the following bijections:
$$\left\{ \begin{matrix} \text{Ab extns } K/\mathbb{Q} \\ \text{s.t. } C_{K/\mathbb{Q}} \mid (N) \end{matrix} \right\} = \left\{ \begin{matrix} \text{Ab extns } K/\mathbb{Q} \\ \text{s.t. } K \subseteq \mathbb{Q}(\zeta_N) \end{matrix} \right\} \leftrightarrow \left\{ \begin{matrix} \text{Quotients of} \\ \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \end{matrix} \right\} \leftrightarrow \left\{ \begin{matrix} \text{Quotients of} \\ (\mathbb{Z}/N\mathbb{Z})^\times \end{matrix} \right\}$$
$$\text{(by KW Theorem)} \qquad\qquad K \longmapsto \mathrm{Gal}(\mathbb{Q}(\zeta_N)/K)$$

- **Artin symbol:** If L/K is abelian extension of number fields, and $P \subset \mathcal{O}_K$ a non-zero prime ideal, and P unramified in $\mathcal{O}_L$, then we define the **Artin symbol** $(P, L/K) \in \mathrm{Gal}(L/K)$ by
$$(P, L/K) := \mathrm{Frob}_{Q/P}, \text{ for any prime ideal } Q \subset \mathcal{O}_L \text{ lying above } P.$$

- **Class field theory over $\mathbb{Q}$:** Let $N \geq 1$ be an integer, and let $K/\mathbb{Q}$ be an abelian extension such that $C_{K/\mathbb{Q}} \mid N$. In particular any prime $p \not| N$ is unramified, so the Artin symbol $((p), K/\mathbb{Q}) \in \mathrm{Gal}(K/\mathbb{Q})$ is defined. Then there is a unique surjective homomorphism $\phi_{K/\mathbb{Q}} : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathrm{Gal}(K/\mathbb{Q})$ given by, for all primes $p \not| N$:
$$\begin{aligned} \phi_{K/\mathbb{Q}} : (\mathbb{Z}/N\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \\ p \bmod N &\longmapsto ((p), K/\mathbb{Q}) \end{aligned}$$

This therefore gives a bijection between the following two sets:

$$\left\{ \begin{array}{c} \text{Abelian extensions } K/\mathbb{Q} \\ \text{such that } C_{K/\mathbb{Q}} \,|\, (N) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Quotients of} \\ (\mathbb{Z}/N\mathbb{Z})^\times \end{array} \right\}$$

$$K \longmapsto \ker \phi_{K/\mathbb{Q}}$$

- **Modulus:** Let K be a number field. A **modulus** is a pair $m = (m_0, m_\infty)$ where
  - $m_0 \subset \mathcal{O}_K$ is a non-zero ideal.
  - $m_\infty \subset \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})$ is possibly empty subset.

  Partial order: If $m = (m_0, m_\infty)$ and $n = (n_0, n_\infty)$ are moduli, we say $m \leq n$ if $m_0 | n_0$ and $m_\infty n_\infty$.

  Fact: Note that $|\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})| = [K : \mathbb{Q}] = r + 2s$ where

$$r = |\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})| \quad \text{and}$$
$$s = \frac{1}{2}|\{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) : \tau(K) \not\subseteq \mathbb{R}\}|$$

- If E/K is any abelian extension, we can define its associated modulus $m_{E/K} = (m_{E/K,0}, m_{E/K,\infty})$ where

$$m_{E/K,0} = C_{E/K}$$
$$m_{E/K,\infty} = \{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R}) : \nexists \tilde{\tau} \in \mathrm{Hom}_{\mathbb{Q}}(E, \mathbb{R}) \text{ s.t. } \tilde{\tau}|_K = \tau\}$$

  (i.e. $m_{E/K,\infty}$ is the set of real embeddings of K which do **not** extend to real embeddings of E)

- **Ideal class group:** Let K be number field. Define

$$\mathcal{I} := \mathrm{Div}\mathcal{O}_k = \{\text{non-zero fractional ideals of } \mathcal{O}_K\}$$
$$\mathcal{P} := \{I \in \mathcal{I} : \exists \alpha \in K^* \text{ s.t. } I = (\alpha)\}$$

  (i.e. $\mathcal{I}$ is the fractional ideals, and $\mathcal{P}$ is the principal fractional ideals) The ideal class group of $\mathcal{O}_K$ is $\mathcal{I}/\mathcal{P}$.

- **Ray class group:** Let $m = (m_0, m_\infty)$ be a modulus. Define

$$k(m_0) = \{\alpha \in K^\times : \forall P \subset O_K, v_p(m_0) > 0 \implies v_p(\alpha) = 0\}$$
$$\mathcal{I}(m_0) = \{I \in \mathcal{I} : \forall P \subset O_K \text{ non-zero prime ideal }, v_p(m_0) > 0 \implies v_p(I) = 0\}$$
$$\mathcal{P}(m_0) = \mathcal{P} \cap \mathcal{I}(m_0)$$

  The ray class group of modulus M is $H(m) = \mathcal{I}(m_0)/\mathcal{P}_m$.

  Properties:
  - $H(m)$ is a finite abelian group.
  - There are short exact sequences:

$$0 \longrightarrow \mathcal{P}(m_0)/\mathcal{P}_m \longrightarrow H(m) \longrightarrow H_k \longrightarrow 0$$

    and

$$0 \longrightarrow \mathcal{O}_k^\times/(\mathcal{O}_k^\times \cap k_m) \longrightarrow (\mathcal{O}_k/m_0)^\times \times \{\pm 1\}^{m_\infty} \longrightarrow \mathcal{P}(m_0)/\mathcal{P}_m \longrightarrow 0$$

    In particular,

$$|H(m)| = |H_K| \cdot |(\mathcal{O}_k/m_0)^\times| \cdot 2^{|m_\infty|} \cdot |\mathcal{O}_k^\times/\mathcal{O}_k^\times \cap k_m|^{-1}$$

Examples:

- If $m = (\mathcal{O}_k,)$ is the trivial modulus, then $H(m) == \mathcal{I}/\mathcal{P}$ is the usual class group.
- $k = \mathcal{Q}$, then the modulus (m_0, m_∞) is such that $m_0 \subset \mathcal{O}_K = \mathbb{Z}$ and $m_\infty \subset \{\mathrm{id}\}$

  Case 1: If $m_0 = (N)$ and $m_\infty = \{id\}$:

$$K(m_0) = \{\alpha \in \mathbb{Q}^\times : p|N \implies p \not|\alpha\}$$
$$K_m = \{\alpha \in K(m_0) : p^k||N \implies p^k|(\alpha - 1) \text{ and } \alpha > 0\}$$

  Thus

$$H(m) \cong \frac{(\mathbb{Z}/N\mathbb{Z})^\times \times \{\pm 1\}}{\mathbb{Z}^\times} \cong (\mathbb{Z}/N\mathbb{Z})^\times$$

  Case 2: If $m_0 = (N)$ and $m_\infty =$: Thus

$$H(m) \cong \frac{(\mathbb{Z}/N\mathbb{Z})^\times}{\mathbb{Z}^\times}$$

- **GCFT:** Let K be a number field, m a modulus of k.

  ..

- **Binary quadratic form:** A polynomial $f(x, y) = ax^2 + bxy + cy^2$ where $a, b, c \in \mathbb{Z}$.

$$\text{Equivalently,} \quad f(x, y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

  We say an integer m is represented by $f(x, y)$ if there exist $x_0, y_0 \in \mathbb{Z}$ such that $f(x_0, y_0) = m$.

Misc

- **Trace:** Let E be a finite extension of K. We have the k-linear map $m_x : E \to E$ where $m_x(y) = xy$ (multiplication by x). We define the trace $\mathrm{Tr}_{E/K} : E \to K$ as $\mathrm{Tr}_{E/K} = \mathrm{tr}(m_x)$ (usual trace of matrix)

  Example: If $k = \mathbb{Q}$, $E = \mathbb{Q}[\sqrt{d}]$, then $\{1, \sqrt{d}\}$ is basis for E over K. If $x = a + b\sqrt{d}$, then $\mathrm{Tr}_{E/k}(x) = 2a$.

- We have $\mathrm{tr}_{E/K}(x) = \sigma_1(x) + \cdots + \sigma_n(x)$ where σ are all K-embeddings of E in $\bar{K}$.

- **Compositum:** The compositum of two fields E, F is the smallest field containing both E and F