Algebraic Number Theory - Chapter I: Integers (Summary)

§ 1. The Gaussian Integers

Ring of Integers: The ring $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ is the integral closure of $\mathbb{Z}$ in the field $\mathbb{Q}(i)$. It consists precisely of the elements in $\mathbb{Q}(i)$ satisfying a monic polynomial in $\mathbb{Z}[x]$.

Prime Elements (up to units):

1. $\pi = 1 + i$ (associated to 2).
2. $\pi = a + bi$ with $a^2 + b^2 = p$, where $p \in \mathbb{Z}$ is a prime with $p \equiv 1 \pmod 4$.
3. $\pi = p$, where $p \in \mathbb{Z}$ is a prime with $p \equiv 3 \pmod 4$.

---

§ 2. Integrality

2.1. Definitions & Transitivity

- **Algebraic Number Field:** Finite extension $K|\mathbb{Q}$.
- **Algebraic Integer:** Root of a monic $f(x) \in \mathbb{Z}[x]$.
- **Integral over** A**:** $b \in B$ is integral over $A \subseteq B$ if it satisfies $x^n + a_1x^{n-1} + \cdots + a_n = 0$ ($a_i \in A$).
- **Integral Closure:** $\overline{A} = \{b \in B \mid b \text{ integral over } A\}$.
- **Normalization:** The integral closure of a domain A in its fraction field.
- **Transitivity (Prop 2.4):** If $A \subseteq B \subseteq C$ are rings, B integral over A, C integral over $B \implies C$ integral over A.

2.2. Row-Column Expansion

Let M be an $r \times r$ matrix, M^* its adjoint. Then $MM^* = \det(M)I$. Implication:

$$Mx = 0 \implies \det(M)x = 0.$$

(Used to prove: finite generation $\iff$ integrality).

2.3. Integrality in Extensions

Let A be an integrally closed domain, $K = \mathrm{frac}(A)$, $L|K$ a finite extension, and B the integral closure of A in L.

- Every $\beta \in L$ can be written as $\beta = b/a$ with $b \in B, a \in A$.
- An element $\beta \in L$ belongs to B if and only if its minimal polynomial over K lies in $A[x]$.

2.4. Trace, Norm, Characteristic Poly.

For $x \in L$, let $T_x : L \to L$ be the map $\alpha \mapsto x\alpha$.

- **Char. Poly:** $f_x(t) = \det(tI - T_x)$.
- **Trace:** $Tr_{L/K}(x) = \mathrm{trace}(T_x)$.
- **Norm:** $N_{L/K}(x) = \det(T_x)$.

If $L|K$ is separable with embeddings $\sigma : L \to \bar{K}$:

$$f_x(t) = \prod_\sigma (t - \sigma x), \quad Tr(x) = \sum_\sigma \sigma x, \quad N(x) = \prod_\sigma \sigma x.$$

Tower Property: $K \subseteq L \subseteq M$.

$$Tr_{M/K} = Tr_{L/K} \circ Tr_{M/L}, \quad N_{M/K} = N_{L/K} \circ N_{M/L}.$$

2.5. Discriminant Calculations

For a basis $\alpha_1, \ldots, \alpha_n$ of $L|K$ (separable):

$$d(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i\alpha_j)^2 = \det(Tr_{L/K}(\alpha_i\alpha_j)).$$

If the basis is $1, \theta, \ldots, \theta^{n-1}$ (power basis):

$$d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \quad \text{(Vandermonde)}.$$

2.6. Bilinear Form

The trace defines a bilinear form $L \times L \to K$:

$$(x, y) \mapsto Tr_{L/K}(xy).$$

It is **non-degenerate** if $L|K$ is separable (i.e., discriminant $\neq 0$). With basis $\{\alpha_i\}$, it corresponds to matrix $M_{ij} = Tr(\alpha_i\alpha_j)$.

2.7. Integrality of Trace and Norm

If A is integrally closed and $x \in B$ (integral closure), then:

$$Tr_{L/K}(x) \in A \quad \text{and} \quad N_{L/K}(x) \in A.$$

Units and Norms: Since the norm is multiplicative, an element $x \in B$ is a unit if and only if its norm is a unit in A:

$$x \in B^\times \iff N_{L/K}(x) \in A^\times.$$

(e.g., for $A = \mathbb{Z}$, x is a unit $\iff N(x) = \pm 1$).

2.8. Localization of the Discriminant

Let $\alpha_1, \ldots, \alpha_n \in B$ be a basis of $L|K$ with discriminant d. Then:

$$dB \subseteq A\alpha_1 + \cdots + A\alpha_n.$$

2.9. Integral Basis

An integral basis is a basis $\omega_1, \ldots, \omega_n$ of $L|K$ such that $B = A\omega_1 + \cdots + A\omega_n$.

- If A is a PID, then every finitely generated submodule $M \neq 0$ of L is a free A-module of rank $[L : K]$. Thus, B admits an integral basis.

2.10. Discriminant of Algebraic Integers

Let $\wr_K$ be the ring of integers of K. The discriminant of K (or an ideal $\mathfrak{a}$) is defined via a $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$ of $\wr_K$ (or $\mathfrak{a}$):

$$d(\mathfrak{a}) = d(\alpha_1, \ldots, \alpha_n).$$

- It is independent of the choice of basis.
- $d(\mathfrak{a}) \neq 0$ implies linear independence.
- Relation: If $\mathfrak{a} \subseteq \mathfrak{a}'$, then $d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 d(\mathfrak{a}')$.

---

§ 3. Ideals

3.1. Dedekind Domains

Theorem 3.1 (Properties of $\mathfrak{o}_K$). The ring of integers $\mathfrak{o}_K$ in a number field K is Noetherian, integrally closed, and every non-zero prime ideal is maximal.

Definition 3.2. An integral domain $\mathfrak{o}$ is called a **Dedekind domain** if it satisfies the following conditions:

1. It is **Noetherian**.
2. It is **integrally closed**.
3. Every non-zero prime ideal is **maximal**.

3.2. Factorization of Integral Ideals

Lemma 3.4. For every ideal $\mathfrak{a} \neq 0$ of a Dedekind domain $\mathfrak{o}$, there exist non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that:

$$\mathfrak{a} \supseteq \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

Definition (Inverse of a Prime). Let $\mathfrak{p}$ be a prime ideal. Define the set:

$$\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subseteq \mathfrak{o}\}.$$

Lemma 3.5. Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}$. For every ideal $\mathfrak{a} \neq 0$:

$$\mathfrak{a}\mathfrak{p}^{-1} := \left\{ \sum a_i x_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1} \right\} \neq \mathfrak{a}.$$

Specifically, $\mathfrak{o} \subsetneq \mathfrak{p}^{-1}$ and $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$.

Theorem 3.3 (Unique Prime Factorization). Every ideal $\mathfrak{a}$ of $\mathfrak{o}$ different from (0) and (1) admits a factorization

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

into non-zero prime ideals $\mathfrak{p}_i$ of $\mathfrak{o}$, which is **unique** up to the order of the factors.

3.3. Fractional Ideals and the Ideal Group

Definition 3.7. A **fractional ideal** of K is a finitely generated $\mathfrak{o}$-submodule $\mathfrak{a} \neq 0$ of K.

Equivalent Definition: An $\mathfrak{o}$-submodule $\mathfrak{a} \subset K$ ($\mathfrak{a} \neq 0$) is a fractional ideal if and only if there exists a non-zero element $c \in \mathfrak{o}$ such that $c\mathfrak{a} \subseteq \mathfrak{o}$ (i.e., $c\mathfrak{a}$ is an integral ideal).

Proposition 3.8 (Ideal Group). The fractional ideals form an abelian group J_K, called the **ideal group** of K.

- **Identity:** $(1) = \mathfrak{o}$.
- **Inverse:** The inverse of $\mathfrak{a}$ is:

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathfrak{o}\}.$$

Corollary 3.9. Every fractional ideal $\mathfrak{a}$ admits a unique representation as a product:

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$$

with $\nu_{\mathfrak{p}} \in \mathbb{Z}$ and $\nu_{\mathfrak{p}} = 0$ for almost all $\mathfrak{p}$. Thus, J_K is the **free abelian group** on the set of non-zero prime ideals $\mathfrak{p}$ of $\mathfrak{o}$.

3.4. The Class Group

Principal Fractional Ideals (P_K). The fractional ideals of the form $(a) = a\mathfrak{o}$ for $a \in K^*$ form a subgroup of J_K denoted by P_K.

Ideal Class Group (Cl_K). The quotient group:

$$Cl_K = J_K / P_K$$

is called the **ideal class group** of K.

Fundamental Exact Sequence: The relation between numbers and ideals is captured by the exact sequence:

$$1 \longrightarrow \mathfrak{o}^* \hookrightarrow K^* \xrightarrow{a \mapsto (a)} J_K \xrightarrow{proj} Cl_K \longrightarrow 1$$

---

§ 4. Extensions of Dedekind Domains

Let o be a Dedekind domain, K its field of fractions, $L|K$ a finite extension, and $\mathcal{O}$ the integral closure of o in L.

4.1. Stability of Dedekind Domains

Proposition: The ring $\mathcal{O}$ is a Dedekind domain.

Proof Sketch (Key Points):

1. **Integrally Closed:** $\mathcal{O}$ is the integral closure by definition.
2. **Krull Dimension 1:** Let $\mathfrak{P}$ be a nonzero prime ideal of $\mathcal{O}$. Then $\mathfrak{p} = \mathfrak{P} \cap o$ is a nonzero prime (maximal) ideal of o. The field extension $\mathcal{O}/\mathfrak{P}$ over $o/\mathfrak{p}$ implies $\mathcal{O}/\mathfrak{P}$ is a field, hence $\mathfrak{P}$ is maximal.
3. **Noetherian:** Condition: If $L|K$ is separable, $\mathcal{O}$ is contained in a finitely generated o-module (via the discriminant), thus $\mathcal{O}$ is a finitely generated o-module (noetherian). (Note: The general case relies on Krull-Akizuki).

4.2. Prime Decomposition and Invariants

Since $\mathcal{O}$ is Dedekind, a nonzero prime ideal $\mathfrak{p} \subset o$ admits a unique factorization in $\mathcal{O}$:

$$\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

We say $\mathfrak{P}_i$ lies over $\mathfrak{p}$ ($\mathfrak{P}_i | \mathfrak{p}$).

Definitions:

- **Ramification Index (e_i):** The exponent $e_i = e(\mathfrak{P}_i | \mathfrak{p})$.
- **Inertia Degree (f_i):** The degree of the residue field extension:
$$f_i = [\mathcal{O}/\mathfrak{P}_i : o/\mathfrak{p}]$$

Classification of Primes:

- **Split Completely:** $e_i = f_i = 1$ for all i, hence $r = [L : K]$.
- **Nonsplit (Indecomposed):** $r = 1$.
- **Unramified:** $e_i = 1$ for all i and all residue extensions $\kappa(\mathfrak{P}_i) | \kappa(\mathfrak{p})$ are separable.
- **Ramified:** There exists some $e_i > 1$ or inseparable residue extension.
- **Totally Ramified:** $r = 1$ and $f_1 = 1$ (implies $e_1 = [L : K]$).

4.3. The Fundamental Identity

Proposition: Condition: If $L|K$ is separable, let $n = [L : K]$. Then:

$$\sum_{i=1}^{r} e_i f_i = n$$

Proof Sketch: Using the Chinese Remainder Theorem:

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_{i=1}^{r} \mathcal{O}/\mathfrak{P}_i^{e_i}$$

We compute the dimension over $\kappa = o/\mathfrak{p}$: 1. $\dim_\kappa(\mathcal{O}/\mathfrak{p}\mathcal{O}) = n$. Since $\mathcal{O}$ is a finitely generated o-module, a basis of $\mathcal{O}/\mathfrak{p}\mathcal{O}$ lifts to a basis of $L|K$. 2. $\dim_\kappa(\mathcal{O}/\mathfrak{P}_i^{e_i}) = e_i f_i$. Considering the filtration $\mathcal{O} \supset \mathfrak{P}_i \supset \cdots \supset \mathfrak{P}_i^{e_i}$, each quotient $\mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1} \cong \mathcal{O}/\mathfrak{P}_i$ has dimension f_i. Summing e_i times gives $e_i f_i$.

4.4. Decomposition via the Conductor

Let $L = K(\theta)$ with $\theta \in \mathcal{O}$. Let $p(x) \in o[x]$ be the minimal polynomial.

Conductor ($\mathfrak{F}$): The largest ideal of $\mathcal{O}$ contained in the ring $o[\theta]$:

$$\mathfrak{F} = \{\alpha \in \mathcal{O} \mid \alpha\mathcal{O} \subseteq o[\theta]\}$$

Proposition (Kummer): Let $\mathfrak{p}$ be a prime of o. Condition: $\mathfrak{p}$ is relatively prime to the conductor ($\mathfrak{p} + \mathfrak{F} = o$). Let $\bar{p}(X) \in (o/\mathfrak{p})[X]$ factor as:

$$\bar{p}(X) = \prod_{i=1}^{r} \bar{p}_i(X)^{e_i}$$

Then the prime decomposition of $\mathfrak{p}$ in $\mathcal{O}$ is $\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ with $f_i = \deg(\bar{p}_i)$.

Key Isomorphisms (Proof Core): The proof relies on the commutative diagram of isomorphisms established by the condition $(\mathfrak{p}, \mathfrak{F}) = 1$:

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong o[\theta]/\mathfrak{p}o[\theta] \cong (o/\mathfrak{p})[X]/(\bar{p}(X))$$

The factorization in the polynomial ring corresponds directly to the decomposition of the ideal.

4.5. Finiteness of Ramification

Proposition: Condition: $L|K$ is separable. There are only finitely many prime ideals of K that ramify in L.

Proof Key: Let $L = K(\theta)$ and $d = \mathrm{disc}(1, \theta, \ldots, \theta^{n-1})$ be the discriminant of the polynomial $p(x)$. A prime $\mathfrak{p}$ is unramified if: 1. $\mathfrak{p} \nmid d$ (implies $\bar{p}(X)$ has simple roots, so all $e_i = 1$). 2. $\mathfrak{p} \nmid \mathfrak{F}$ (allows using the conductor proposition). Since $d \neq 0$ and $\mathfrak{F} \neq 0$, only finitely many primes divide d or are not coprime to $\mathfrak{F}$.