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

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. 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).

3. Integrality in Extensions

Let A be an integrally closed domain, $K = \text{frac}(A)$, $L|K$ 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 $A[x]$.

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:** $Tr_{L/K}(x) = \text{trace}(T_x)$.
- **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: $K \subseteq L \subseteq M$.

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

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):

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

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 $M_{ij} = Tr(\alpha_i\alpha_j)$.

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 $\iff N(x) = \pm 1$).

8. Localization of the Discriminant

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

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

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.

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 $d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 d(\mathfrak{a}')$.