

Number Theory

Book 1

$$J(x) = Li(x) - \sum_{\rho} Li(x^{\rho}) - \log(2) + \int_x^{\infty} \frac{1}{t(t^2 - 1)\log(t)} dt$$

Rational integers ("ordinary integers") $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$

(Algebraic) integers: A number $\alpha \in \mathbb{C}$ is algebraic if it is a root of a nonzero poly. with coefficients in \mathbb{Q}

i.e. $f(\alpha) = 0$ for some $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$, $a_i \in \mathbb{Q}$ i.e. $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$, $a_i \in \mathbb{Z}$ not all zero.

eg. $\frac{\sqrt{2}}{7}$ is algebraic since it's a root of $x^2 - \frac{2}{49} \in \mathbb{Q}[x]$ or $49x^2 - 2 \in \mathbb{Z}[x]$.

We say α is an (algebraic) integer if α is a root of a monic poly. with coefficients in \mathbb{Z} i.e.

$f(\alpha) = 0$ for some $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$, $a_i \in \mathbb{Z}$

eg. $\sqrt{2}$ is integral (it's an ^(algebraic) integer)

If $\mathcal{O} = \{\alpha \in \mathbb{C} : \alpha \text{ is an algebraic integer}\} \subset \mathcal{A} \subset \mathbb{C}$

$\mathcal{A} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic}\} \subset \mathbb{C}$

\mathcal{O} is the ring of alg. int.

\mathcal{A} is the field of alg. numbers.

$\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$ (the rational integers are the ordinary integers).

Fermat's equation: $x^2 - 5y^2 = 1$ has infinitely many ^(ordinary) integer solutions.

$x^2 - 5y^2 = 1 \iff (x + y\sqrt{5})(x - y\sqrt{5}) = 1$ where $x + y\sqrt{5} \in \mathcal{O}$ has Norm is $N(x + y\sqrt{5}) = (x + y\sqrt{5})(x - y\sqrt{5}) = x^2 - 5y^2$

$N(\alpha\beta) = N(\alpha)N(\beta)$ so if $\alpha = 9 + 4\sqrt{5}$ then $N(\alpha) = 9^2 - 5 \cdot 4^2 = 1$ so $N(\alpha^k) = N(\alpha)^k = 1^k = 1$

eg. $(9 + 4\sqrt{5})^2 = 81 + 80 + 72\sqrt{5} = 161 + 72\sqrt{5}$ also has norm 1 so $161^2 - 5 \cdot 72^2 = 1$

$(9 + 4\sqrt{5})^3 = (161 + 72\sqrt{5})(9 + 4\sqrt{5}) = 2889 + 1292\sqrt{5}$

\mathcal{A} is the fraction field of \mathcal{O} i.e. $\mathcal{A} = \{\frac{\alpha}{\beta} : \alpha, \beta \in \mathcal{O}, \beta \neq 0\}$

$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$.

eg. $\sqrt{2}, \sqrt{3} \in \mathcal{O}$ (root of $x^2 - 2$, $x^2 - 3$ respectively)

$\Rightarrow \sqrt{2} \cdot \sqrt{3} = \sqrt{6} \in \mathcal{O}$ (root of $x^2 - 6$)

$\sqrt{2} + \sqrt{3} \in \mathcal{O}$ (root of $x^2 - 10x^2 + 1$)

the min. poly. of $\sqrt{2} + \sqrt{3}$ over \mathbb{Q} .

x	y
1	8
±9	±4
±161	±72
±2889	±1292
⋮	⋮

$$\begin{aligned} x &= \sqrt{2} + \sqrt{3} \\ x^2 &= 5 + 2\sqrt{6} \\ x^2 - 5 &= 2\sqrt{6} \\ x^4 - 10x^2 + 25 &= 24 \\ x^2 - 10x^2 + 1 &= 0 \end{aligned}$$

Let $\alpha \in \mathbb{C}$. If α is algebraic then it has a minimal poly. over \mathbb{Q} i.e. $m(x) \in \mathbb{Q}[x]$ is monic with $m(\alpha) = 0$ and $\deg m(x)$ is as small as possible. In this case $m(x)$ is unique. All polynomials in $\mathbb{Q}[x]$ having α as a root are multiples of $m(x)$.

$$(m(x)) = \{h(x)m(x) : h(x) \in \mathbb{Q}[x]\}$$

$\mathbb{Q}[x]$ is a principal ideal ring (every ideal is principal).

Review: Let R be a commutative ring with identity $1 \in R$. (eg. \mathbb{Z} , $\mathbb{Q}[x]$).

An ideal is a subset $J \subseteq R$, $0 \in J$ such that J is closed under R -linear combinations i.e. $ra + sb \in J$ for all $r, s \in R$, $a, b \in J$. (Every ideal is a subring but not conversely).

Given $a_1, \dots, a_k \in R$, these elements generate an ideal $(a_1, a_2, \dots, a_k) = \{r_1 a_1 + r_2 a_2 + \dots + r_k a_k : r_1, \dots, r_k \in R\} \subset R$.

eg. in \mathbb{Z} , $(2, 6) = \{2r + 6s : r, s \in \mathbb{Z}\} = (3)$

Every ideal in \mathbb{Z} is principal i.e. generated by a single element.

Return to previous setting $\alpha \in \mathbb{C}$ algebraic.

There is a ring homomorphism $\mathbb{Q}[x] \rightarrow \mathbb{C}$

$$f(x) \mapsto f(\alpha)$$

with kernel $J = \{f(x) \in \mathbb{Q}[x] : f(\alpha) = 0\} \subset \mathbb{Q}[x]$ an ideal.

Since α is algebraic, $J = (m(x))$ with $m(x) \neq 0$. Scale $m(x)$ if needed to get $m(x)$ monic. Then $m(x)$ is unique; it's the minimal poly. of α over \mathbb{Q} .

$\mathbb{Z}[x]$ is not a principal ideal ring

$\mathbb{Q}[x, y]$

In $\mathbb{Q}[x, y]$, $(x^2, xy, y^2) = \{f(x, y) \in \mathbb{Q}[x, y] \text{ with no const. term, no } x \text{ term, no } y \text{ term}\}$ is a non-principal ideal.

This ideal cannot be generated by 1 or 2 generators; you need at least 3 generators to generate it.

In $\mathbb{Q}[x, y]$, every ideal is finitely generated (there is a finite list of generators) (Hilbert's basis theorem)

In number theory, a number field ^(algebraic) is a finite extension $K \supseteq \mathbb{Q}$ eg. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \supset \mathbb{Q}$ is a quadratic extension.

$[K:\mathbb{Q}]$ = degree of the extension

$[E:F]$ = degree of field extension $E \supseteq F$ (F subfield of E)
= dimension of E as a vector space over F

$[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}] = 2$ since $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}[\sqrt{2}]$ over \mathbb{Q} .

$\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q}$

$[\mathbb{C}:\mathbb{R}] = 2$

$[\mathbb{C}:\mathbb{Q}] = \infty$

$[\mathbb{R}:\mathbb{Q}] = \infty$.

$K \supseteq \mathbb{Q}$ finite extension $n = [K:\mathbb{Q}] < \infty$. All elements $\alpha \in K$ are algebraic i.e. $K \subset \mathcal{A} = \{\text{algebraic numbers}\}$.

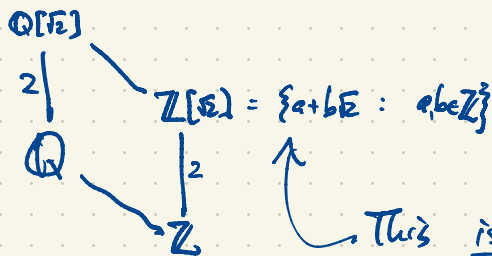
If $\alpha \in K$ then $1, \alpha, \alpha^2, \dots, \alpha^n$ so there exist $a_0, a_1, \dots, a_n \in \mathbb{Q}$ not all zero, s.t. $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$
so α is algebraic. (of degree $\leq n$). The degree of an algebraic number is the degree of its min. poly. = $[\mathbb{Q}(\alpha):\mathbb{Q}]$



$\mathcal{O} = \{\text{alg. integers in } K\}$

$K = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in \mathcal{O}, \beta \neq 0 \right\}$.

eg.



This is a principal ideal ring.

$\mathcal{O} = \{r_1\alpha_1 + \dots + r_n\alpha_n : r_i \in \mathbb{Z}\}$

$\alpha_1, \dots, \alpha_n$ base for $\mathcal{O} \supseteq \mathbb{Z}$

$\alpha_1, \dots, \alpha_n$ basis for $K \supseteq \mathbb{Q}$

\mathcal{O} is not always (usually) a principal ideal ring.

Every ideal $J \subset \mathcal{O}$ has the form

$J = (a)$ or (a, b)

$\mathbb{Z}[\sqrt{2}]$ has infinitely many units

$$(3+2\sqrt{2})^n (3-2\sqrt{2})^n = 1$$

units in $\mathbb{Z}[\sqrt{2}]$

$$\mathbb{Z}[\sqrt{2}]^\times = \{\pm (3+2\sqrt{2})^n : n \in \mathbb{Z}\} \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$$

Ex. $\mathbb{Q}[\sqrt{5}] \supset \mathbb{Q}$ is another quadratic extension (quadratic number field i.e. $[\mathbb{Q}[\sqrt{5}]:\mathbb{Q}] = 2$)
 $\{1, \sqrt{5}\}$ basis for the extension

$\mathbb{Q}[\sqrt{5}]$

$$\mathbb{Z} \mid \mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$$



\mathbb{O}_K (commutative ring with identity)

$\alpha \in \mathbb{O}^* = \{\text{units of } \mathbb{O}\}$ iff $\alpha\beta = 1$ for some $\beta \in \mathbb{O}$.

\mathbb{O}^* is a multiplicative group (abelian).

The only units in $\mathbb{Z}[\sqrt{5}]$ are $\mathbb{Z}[\sqrt{5}]^* = \{\pm 1\}$.

The norm of $\alpha \in \mathbb{Z}[\sqrt{5}]$ is $N(\alpha) = \alpha\bar{\alpha}$, $\overline{a + b\sqrt{5}} = a - b\sqrt{5}$

$$= (a + b\sqrt{5})(a - b\sqrt{5})$$

$$\text{For } \alpha, \beta \in \mathbb{Z}[\sqrt{5}], \quad N(\alpha\beta) = N(\alpha)N(\beta) = (a^2 + 5b^2)(c^2 + 5d^2)$$

$$= (a\bar{a})(b\bar{b}) \quad (c\bar{c})(d\bar{d})$$

If $\alpha = a + b\sqrt{5} \in \mathbb{Z}[\sqrt{5}]^*$ then $N(\alpha) = a^2 + 5b^2 \in \{0, 1, 2, 3, \dots\}$ since $a, b \in \mathbb{Z}$.

$$\alpha\beta = 1 \text{ for some } \beta \in \mathbb{Z}[\sqrt{5}]$$

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1 \Rightarrow N(\alpha) = N(\beta) = 1$$

$\alpha \in \mathbb{Z}[\sqrt{5}]$

$$a^2 + 5b^2 \Rightarrow (a, b) = (\pm 1, 0) \Rightarrow \alpha = \pm 1.$$

α is reducible if $\alpha = \alpha_1\alpha_2$, $\alpha_1, \alpha_2 \in \mathbb{Z}[\sqrt{5}]$, neither α_1 nor α_2 is a unit.

α is irreducible if $\left\{ \begin{array}{l} \text{the only way to factor } \alpha = \alpha_1\alpha_2, \alpha_1, \alpha_2 \in \mathbb{Z}[\sqrt{5}] \\ \text{and } \alpha \text{ is not a unit} \end{array} \right.$ is if one of α_1, α_2 is a unit.

\mathbb{Z} has unique factorization

$$12 = 2 \times 2 \times 3$$

$$= (-2) \times 2 \times (-3)$$

$$= 2 \times 3 \times 2$$

$$= (-2) \times 3 \times (-2)$$

\mathbb{Z} has irreducible elements

$$\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \dots$$

\mathbb{Z} has units ± 1 (invertible elements)

In $\mathbb{Z}[\sqrt{5}]$, 2 is irreducible. $2 \neq \pm 1$.

If $2 = \alpha\beta$, $4 = N(2) = N(\alpha\beta) = N(\alpha)N(\beta)$

$$\begin{array}{|c|} \hline 4 \times 1 \\ \hline 2 \times 2 \\ \hline 1 \times 4 \\ \hline \end{array}$$

β is a unit.
 α unit.

$$N(a+b\sqrt{5}) = a^2 + 5b^2 \in \{0, 1, 2, 3, \dots\}$$

$$N(2) = 4$$

If $N(\alpha) = N(a+b\sqrt{5}) = 1$ then $(a,b) = (\pm 1, 0)$, $\alpha = \pm 1$ is a unit.

So 2 is irreducible in $\mathbb{Z}[\sqrt{5}]$.

4 is reducible. $4 = 2 \times 2$

5 is reducible. $5 = (\sqrt{5})(-\sqrt{5})$

6 is reducible: $6 = 2 \times 3 = (1+\sqrt{5})(1-\sqrt{5})$ where all 2, 3, $1 \pm \sqrt{5}$ are irreducible by proof similar to above.

$\mathbb{Z}[\sqrt{5}]$ does not have unique factorization of elements.

But: ideals in $\mathcal{O} \subset K$ (K any alg. number field) always have unique factorization.)

Proof(?) of FLT for exponent 3, say: If x, y, z positive integers with $x^3 + y^3 = z^3$

$$(x+y)(x+\omega y)(x+\omega^2 y) = z^3, \quad \omega = e^{2\pi i/3} = \frac{-1 + \sqrt{-3}}{2} \text{ is an algebraic integer}$$

$\mathbb{Z}[\omega]$ has unique factorization