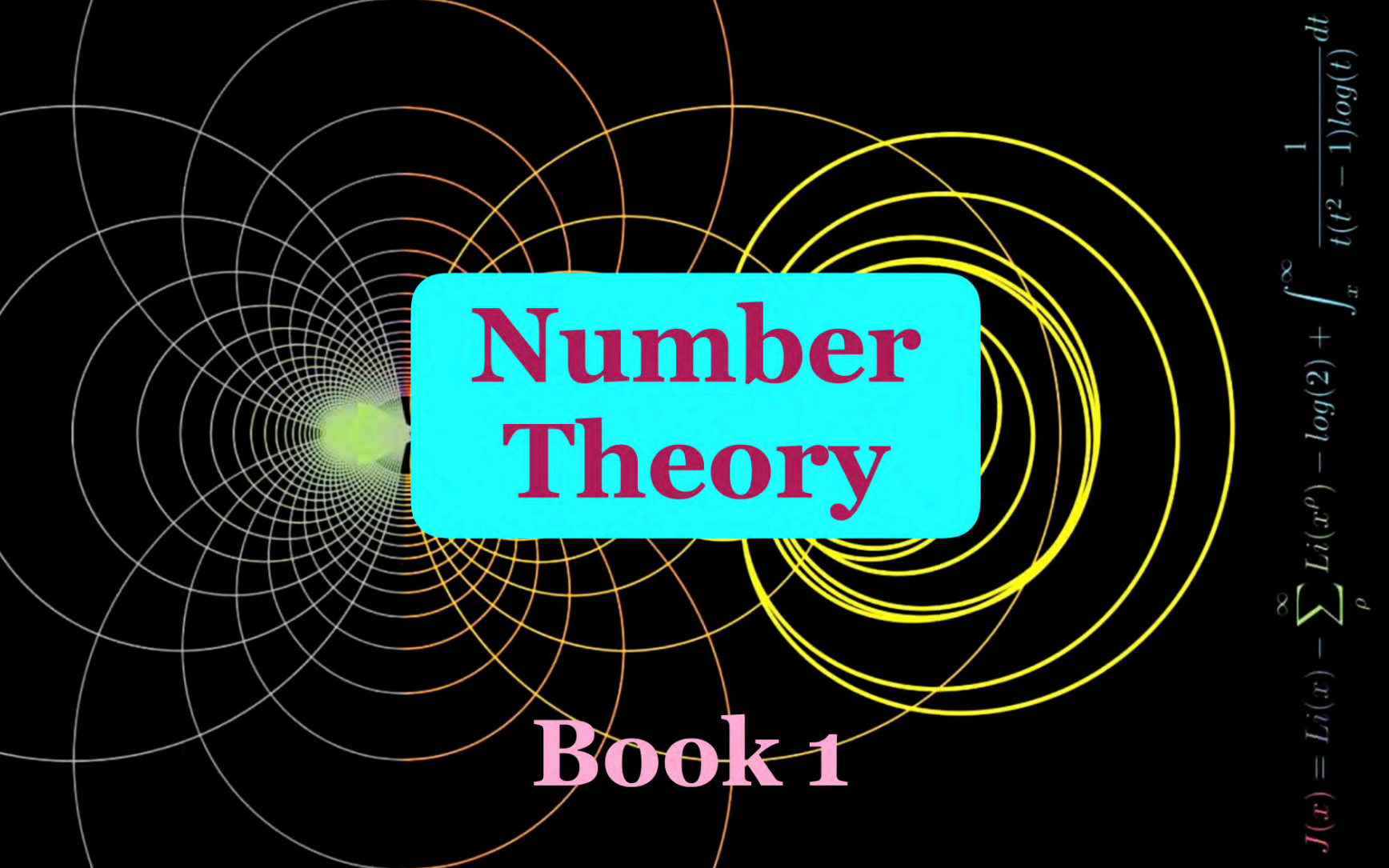

Number
Theory
Book 1
$J(x) = Li(x) - \sum_{\rho} Li(x^{\rho}) - \log(2) + \int_x^{\infty} \frac{1}{t(t^2-1)\log(t)} dt$

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 <u>algebraic</u> if it is a root of a nonzero poly. with coefficients in $\mathbb{Q}$

i.e. $f(\alpha) = 0$ for some $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_i \in \mathbb{Q}$ i.e. $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_i \in \mathbb{Z}$ 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 (<u>algebraic</u>) <u>integer</u> if α is a root of a <u>monic</u> poly. with coefficients in $\mathbb{Z}$ ie.

$f(\alpha) = 0$ for some $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_i \in \mathbb{Z}$.

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 <u>ring</u> of alg. int.

$\mathcal{A}$ is the <u>field</u> of alg. numbers.

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

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

x	y
1	0
± 9	± 4
± 161	± 72
± 2889	± 1292
⋮	⋮

$x^2 - 5y^2 = 1 \iff (x + y\sqrt{5})(x - y\sqrt{5}) = 1$ 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 $\mathcal{O}$ ie. $\mathcal{A} = \{\frac{\alpha}{\beta} : \alpha, \beta \in \mathcal{O}, \beta \neq 0\}$

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

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

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

$\sqrt{2} + \sqrt{3} \in \mathcal{O}$ (root of $x^4 - 10x^2 + 1$)

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

$x = \sqrt{2} + \sqrt{3}$

$x^2 = 5 + 2\sqrt{6}$

$x^2 - 5 = 2\sqrt{6}$

$x^4 - 10x^2 + 25 = 24$

$x^4 - 10x^2 + 1 = 0$

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 $(a_1, a_2, \dots, a_k) = \{ r_1a_1 + r_2a_2 + \cdots + r_ka_k : r_1, \dots, r_k \in R \} \subset R$.

eg. in $\mathbb{Z}$, $(21, 6) = \{ 21r + 6s : r, s \in \mathbb{Z} \} = (3)$

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

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

There is a ring homomorphism $\mathbb{Q}[x] \longrightarrow \mathbb{C}$, $f(x) \longmapsto f(\alpha)$ with kernel $J = \{ f(x) \in \mathbb{Q} : f(\alpha) = 0 \} \subset \mathbb{Q}[x]$ 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 $\mathbb{Q}[x, y]$, $(x^2, xy, y^2) = \{ f(x, y) \in \mathbb{Q}[x, y]$ with no const. term, no x term, no y 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 (algebraic) field is a finite extension $K \geq \mathbb{Q}$ 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 $\mathbb{Q}$.

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

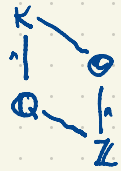
$[\mathbb{C}:\mathbb{R}] = 2$

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

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

$K \supseteq \mathbb{Q}$ 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. $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$
so α is algebraic. (of degree $\le n$. The degree of an algebraic number is the degree of its min. poly. $= [\mathbb{Q}(\alpha):\mathbb{Q}]$



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

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

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

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

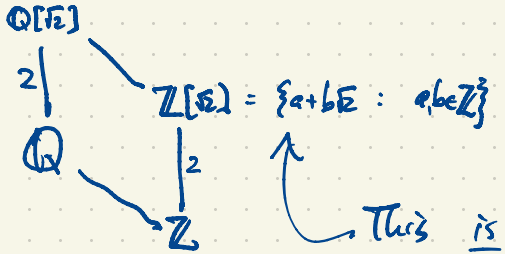
$\alpha_1, \dots, \alpha_n$ basis for $K \supseteq \mathbb{Q}$

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

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

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

eg.



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

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

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

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

Eg. $\mathbb{Q}[\sqrt{-5}] \supset \mathbb{Q}$ is another quadratic extension (quadratic number field i.e. $[\mathbb{Q}[\sqrt{-5}] : \mathbb{Q}] = 2$)

$\{1, \sqrt{-5}\}$ basis for the extension

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

2 | $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$

$\mathbb{Q}$ | $\mathbb{Z}$

$\mathbb{Z}$ 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 $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \ldots$

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

In $\mathcal{O}$ (commutative ring with identity)

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

$\mathcal{O}^\times$ is a multiplicative group (abelian).

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

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

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

$= a^2 + 5b^2$.

For $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$, $N(\alpha\beta) = N(\alpha)N(\beta)$.

$(\alpha\beta)(\overline{\alpha\beta})$ " $(\alpha\bar{\alpha})(\beta\bar{\beta})$ "

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

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

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

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

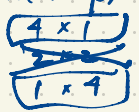
$\alpha \in \mathbb{Z}[\sqrt{-5}]$

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

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

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



β is a unit. α unit

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

$N(2) = 4$

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

$N(\alpha) = a^2 + 5b^2 = 2$ has no solution for $a, b \in \mathbb{Z}$

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

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

5 " " $5 = (\sqrt{-5})(-\sqrt{-5})$

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.) Aside

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

$(x+y)(x+\omega y)(x+\omega^2 y) = z^3$, $\omega = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$ is an algebraic integer $\mathbb{Z}[\omega]$ has unique factorization

In $\mathbb{Z}[\sqrt{-5}]$, we don't have unique factorization of elements but we do have unique factorization of ideals.

$(a) = \{ra : r \in \mathbb{Z}[\sqrt{-5}]\}$

$(a,b) = \{ra + sb : r, s \in \mathbb{Z}[\sqrt{-5}]\}$ etc.

$(6) = (2)(3) = (1+\sqrt{-5})(1-\sqrt{-5}) = \mathfrak{p}^2\mathfrak{q}\bar{\mathfrak{q}}$ where $\mathfrak{p}, \mathfrak{q}, \bar{\mathfrak{q}} \subset \mathbb{Z}[\sqrt{-5}]$ are prime ideals. (not principal)

not prime factors

$(2) = \mathfrak{p}^2$

$(3) = \mathfrak{q}\bar{\mathfrak{q}}$

$(1+\sqrt{-5}) = \mathfrak{p}\mathfrak{q}$

$(1-\sqrt{-5}) = \mathfrak{p}\bar{\mathfrak{q}}$

$\mathfrak{p} = (2, 1+\sqrt{-5})$

$\mathfrak{q} = (3, 1+\sqrt{-5})$

$\bar{\mathfrak{q}} = (3, 1-\sqrt{-5})$

If $\mathcal{A}, \mathcal{B} \subseteq R$ are ideals then $\mathcal{A}+\mathcal{B}$, $\mathcal{A}\cap\mathcal{B}$, $\mathcal{AB} \subseteq R$ are ideals.

$\mathcal{A}+\mathcal{B} = \{\alpha+\beta : \alpha\in\mathcal{A}, \beta\in\mathcal{B}\}$.

$\mathcal{AB}$ is not simply $\{\alpha\beta : \alpha\in\mathcal{A}, \beta\in\mathcal{B}\}$ is not an ideal in general because it's not closed under $\pm$.

$\mathcal{AB}$ = closure of $\{\alpha\beta : \alpha\in\mathcal{A}, \beta\in\mathcal{B}\}$ under $\pm$.

$= \{r_1\alpha_1\beta_1 + r_2\alpha_2\beta_2 + \cdots + r_k\alpha_k\beta_k : k\geq 1,\ r_i\in R,\ \alpha_i\in\mathcal{A},\ \beta_i\in\mathcal{B}\}$.

eg. $\mathfrak{p} = (2, 1+\sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$

$= \{2r + (1+\sqrt{-5})s : r,s\in\mathbb{Z}[\sqrt{-5}]\}$.

$\mathfrak{p}^2 = (4,\ 2(1+\sqrt{-5}),\ \underbrace{(1+\sqrt{-5})^2}_{-4+2\sqrt{-5}}) \subseteq (2)$

$2 = \underbrace{(1+\sqrt{-5})}_{\mathfrak{p}}\underbrace{(1-\sqrt{-5})}_{2-(1+\sqrt{-5})} + 2\cdot\underbrace{(-2)}_{\mathfrak{p}\,\mathfrak{p}} \in \mathfrak{p}^2 \Rightarrow (2)\subseteq\mathfrak{p}^2$

$(2) = \mathfrak{p}^2$.

$\bar{\mathfrak{p}} = (2, \underbrace{1-\sqrt{-5}}_{2-(1+\sqrt{-5})}) = \mathfrak{p}$

$\mathfrak{q} = (3, 1+\sqrt{-5})$

$\bar{\mathfrak{q}} = (3, 1-\sqrt{-5})$

$\mathfrak{q}\bar{\mathfrak{q}} = (9,\ 3(1-\sqrt{-5}),\ 3(1+\sqrt{-5}),\ 6) \subseteq (3)$

$3 = 3\cdot 3 - (1+\sqrt{-5})(1-\sqrt{-5}) \in \mathfrak{q}\bar{\mathfrak{q}} \Rightarrow (3)\subseteq\mathfrak{q}\bar{\mathfrak{q}}$

$\Rightarrow (3) = \mathfrak{q}\bar{\mathfrak{q}}$

$\mathfrak{p} = (2, 1+\sqrt{-5})$

$\mathfrak{q} = (3, 1+\sqrt{-5})$

$1+\sqrt{-5} = (-2)(1+\sqrt{-5}) + (1+\sqrt{-5})(3) \in \mathfrak{p}\mathfrak{q}$

$(1+\sqrt{-5}) \subseteq \mathfrak{p}\mathfrak{q}$

$\mathfrak{p}\mathfrak{q} = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) = (6,\ 2(1+\sqrt{-5}),\ 3(1+\sqrt{-5}),\ \underbrace{(1+\sqrt{-5})^2}_{(1+\sqrt{-5})(1-\sqrt{-5})}) \subseteq (1+\sqrt{-5})$

$\mathfrak{p}\mathfrak{q} = (1+\sqrt{-5})$

$\mathfrak{p}\bar{\mathfrak{q}} = \overline{\mathfrak{p}\mathfrak{q}} = (1-\sqrt{-5})$

$\bar{\mathfrak{p}} = \mathfrak{p}$

In $\mathbb{Z}$, "prime" usually means "positive irreducible" i.e. $2, 3, 5, 7, 11, 13, \ldots$ (Irreducibles are $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \ldots$)

In alg. no. theory we refer to prime ideals and irreducible elements.

Let K be a (alg) no. field i.e. a finite extension $K \supseteq \mathbb{Q}$, $n = [K:\mathbb{Q}]$ = degree of the extension $< \infty$

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

$K = \{r_1\alpha_1 + \cdots + r_n\alpha_n : r_i \in \mathbb{Q}\}$

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

n | $\mathbb{Q}$ — $\mathbb{Z}$ | n

$\mathcal{O}$ has unique factorization of ideals but not necessarily of elements.

An ideal $\mathfrak{p} \subset \mathcal{O}$ is prime if $a,b \in \mathcal{O}$, $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Nonzero prime ideals $\mathfrak{p} \subset \mathcal{O}$ are maximal.

If R is a commutative ring with identity and $A \subseteq R$ is an ideal, A is maximal if $A \subset R$ (proper containment, $A \neq R$) and there is no ideal B with $A \subset B \subset R$.

$\Leftrightarrow$ R/A is a field.

A is prime if $a,b \in R$, $ab \in A \Rightarrow a \in A$ or $b \in A$

$\Leftrightarrow$ R/A is an integral domain. (no zero divisors)

Maximal $\Rightarrow$ Prime.

Usually the converse is very far from true e.g. in $R = \mathbb{Q}[x,y]$ the ideal $(x) \subset R$ is prime. $R/(x) \cong \mathbb{Q}[y]$ is an integral domain. But $\mathbb{Q}[y]$ is not a field so $(x) \subset R$ is not maximal.

$(x) \subset (x,y) \subset R$ where $(x,y) = \{f(x,y) \in R : f(0,0) = 0\} \subset R$ is maximal

$R/(x,y) \cong \mathbb{Q}$ is a field.

In $\mathcal{O}$, if $A \subset \mathcal{O}$ is a nonzero ideal then A maximal iff A is prime.

("Nonzero primes are maximal.")

How are prime ideals in $\mathbb{Z}$ i.e. $(p) \subset \mathbb{Z}$ related to prime ideals $\mathfrak{p} \subset \mathcal{O}$?

Every prime ideal $\mathfrak{p} \subset \mathcal{O}$ contains a unique prime ideal $(p) \subset \mathbb{Z}$

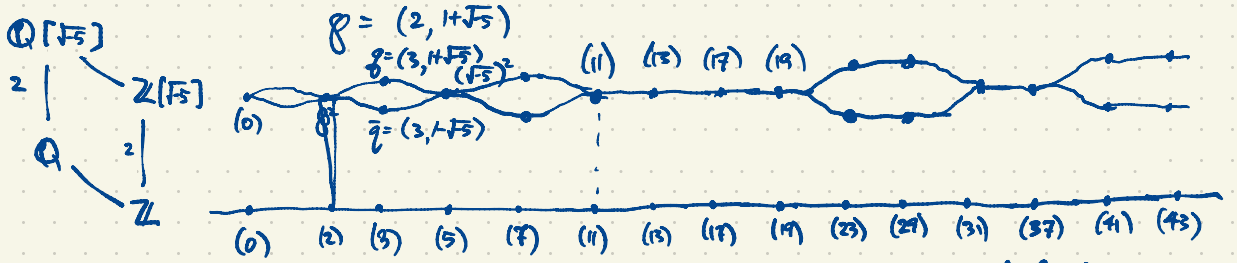
$\mathfrak{p} \cap \mathbb{Z} \subset \mathbb{Z}$ prime

$\mathfrak{p} \cap \mathbb{Z} = (p) \subset \mathbb{Z}$, p ordinary prime (rational prime)

In other direction, given a prime ideal $(p) \subset \mathbb{Z}$, this gives an ideal $(p) \subset \mathcal{O}$ may or may not be prime.

$\parallel$

$p\mathcal{O}$



prime ideals of $\mathbb{Z}$ $\quad$ $\operatorname{Spec}\mathbb{Z} = \{\text{prime ideals of } \mathbb{Z}\}$

$5 = (\sqrt{-5})(-\sqrt{-5})$

To figure out how rational primes p behave in an extension:
they either ramify $(2,5)$
or split
or remain prime.

Think about what happens to a poly. ring like $\mathbb{R}[x]$ in a quadratic extension.

Take $f(x) \in \mathbb{R}[x]$ a poly. of degree 2 and consider $\mathbb{R}[x]/(f(x))$.

(i) If $f(x) \in \mathbb{R}[x]$ is irreducible eg. x^2+1 then $(f(x)) \subset \mathbb{R}[x]$ is maximal and $\mathbb{R}[x]/(f(x)) \cong \mathbb{C}$

(ii) If $f(x) \in \mathbb{R}[x]$ has two distinct real roots, say $f(x) = (x-a)(x-b)$, $a \neq b$, then

$$\mathbb{R}[x]/((x-a)(x-b)) = \mathbb{R}[x]/((x-a)\cap(x-b)) \cong \mathbb{R}[x]/(x-a) \oplus \mathbb{R}[x]/(x-b) \cong \mathbb{R} \oplus \mathbb{R}$$

(iii) If $f(x) \in \mathbb{R}[x]$ has a double real root eg. $f(x) = x^2$ or $(x-a)^2$ $\quad \mathbb{R}[x]/(x^2) = \{a + b\underset{\varepsilon}{x} : a,b \in \mathbb{R}\}$ is the ring of dual numbers over $\mathbb{R}$

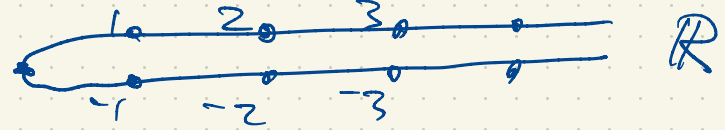
$(a+b\varepsilon)(c+d\varepsilon) = ac + (ad+bc)\varepsilon$

(i): $(f(x)) \subset \mathbb{R}[x]$ is maximal (remains prime)

(ii) $(f(x)) = (x-a)(x-b)$ splits $(x-a), (x-b) \subset \mathbb{R}[x]$ prime.

(iii) $(f(x)) = (x-a)^2$ ramifies

Squaring $\mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$



$\mathbb{Z}[x] \to \mathbb{Z}[\sqrt{-5}]$, $f(x) \mapsto f(\sqrt{-5})$

$\mathbb{Z}[x]/(x^2+5)$

In $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$, what happens to an ordinary prime $p \in \mathbb{Z}$ in this extension? We should look at

$$\mathcal{O}/p\mathcal{O} \cong \frac{\mathbb{Z}[x]/(x^2+5)}{p\mathbb{Z}[x]/(x^2+5)} \cong \mathbb{Z}[x]/(p, x^2+5) \cong \mathbb{F}_p[x]/(x^2+5)$$

where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0,1,2,\dots,p-1\}$ field of order p.

use the isomorphism theorems for ring theory

Try a few primes $p \in \mathbb{Z}$

$\mathcal{O}/2\mathcal{O} \cong \mathbb{F}_2[x]/(x^2+5) = \mathbb{F}_2[x]/(x^2+1)$

$\mathcal{O}/2\mathcal{O} \cong \mathbb{F}_2[x]/(x^2+5) \cong \mathbb{F}_2[\varepsilon]$ dual numbers

$x^2+1 \in \mathbb{F}_2[x]$ ramifies: $x^2+1 = (x+1)^2$

So the rational prime $2 \in \mathbb{Z}$ ramifies in $\mathcal{O}$ as $(2) = 2\mathcal{O} = \mathfrak{g}^2$ for some prime ideal $\mathfrak{g} \subset \mathcal{O}$.

(From before: $\mathfrak{g} = (2, 1+\sqrt{-5})$)

$\mathcal{O}/3\mathcal{O} \cong \mathbb{F}_3[x]/(x^2+5) \cong \mathbb{F}_3[x]/(x^2+2) \cong \mathbb{F}_3[x]/(x^2-1)$

$x^2+2 = x^2-1 = (x+1)(x-1)$ has two distinct roots in $\mathbb{F}_3$.

So $(3) = 3\mathcal{O} = \mathfrak{q}\mathfrak{q}'$ where $\mathfrak{q} \neq \mathfrak{q}'$ are distinct prime ideals in $\mathcal{O}$.

$\mathcal{O}/3\mathcal{O} \cong \mathbb{F}_3 \oplus \mathbb{F}_3$

(From before $\mathfrak{q} = (3, 1+\sqrt{-5})$, $\mathfrak{q}' = \overline{\mathfrak{q}} = (3, 1-\sqrt{-5})$)

We say (3) splits in $\mathcal{O}$. 3 is an irreducible element in $\mathcal{O}$ but the ideal splits.)

$\mathcal{O}/5\mathcal{O} = \mathbb{F}_5[x]/(x^2+5) \cong \mathbb{F}_5[x]/(x^2) \cong \mathbb{F}_5[\varepsilon]$ dual numbers $x^2 = x \cdot x$

so $(5) = 5\mathcal{O} = (\sqrt{-5})^2$ ramifies

$5 = (\sqrt{-5})(-\sqrt{-5})$

$(5) = (\sqrt{-5})^2$ since $-1 \in \mathcal{O}^\times$

$\mathcal{O}/7\mathcal{O} = \mathbb{F}_7[x]/(x^2+5) = \mathbb{F}_7[x]/(x-2)(x-4) \cong \mathbb{F}_7 \oplus \mathbb{F}_7$ $\quad x^2-2 = (x-3)(x-4)$ $\quad (x^2-2)$ splits

the ideal $(7) = \mathfrak{R}\mathfrak{R}'$ $\quad \mathfrak{R} \neq \mathfrak{R}'$ distinct prime ideals in $\mathcal{O}$

$7\mathcal{O}$ splits

$\mathcal{O}/11\mathcal{O} \cong \mathbb{F}_{11}[x]/(x^2+5) = \mathbb{F}_{11}[x]/(x^2-6) \cong \mathbb{F}_{121}$

$\mathcal{O} = \mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} : a,b \in \mathbb{Z}\}$

In $\mathbb{F}_{11}$

a	a^2
0	0
± 1	1
± 2	4
± 3	9
± 4	5
± 5	3

$x^2-6 \in \mathbb{F}_{11}[x]$ is irreducible

The ideal $(x^2-6) \subset \mathbb{F}_{11}[x]$ is maximal so it's prime.

$(11) = 11\mathcal{O} \subset \mathcal{O}$ is prime

11 remains prime in $\mathcal{O}$.

In $\mathbb{F}_{13}$

a	a^2
0	0
± 1	1
± 2	4
± 3	9
± 4	3
± 5	12
± 6	10

$\mathcal{O}/13\mathcal{O} \cong \mathbb{F}_{13}[x]/(x^2+5) = \mathbb{F}_{13}[x]/(x^2-8) \cong \mathbb{F}_{169}$

$(13) = 13\mathcal{O} \subset \mathcal{O}$ is prime

13 remains prime in $\mathcal{O}$

$\mathcal{O}/17\mathcal{O} \cong \mathbb{F}_{17}[x]/(x^2+5) = \mathbb{F}_{17}[x]/(x^2-12) \cong \mathbb{F}_{289}$

In $\mathbb{F}_{17}$ the squares are $0, 1, 4, 9, 16, 8, 2, 15, 13$.

$x^2-12 \in \mathbb{F}_{17}[x]$ irreducible

$(x^2-12) \subset \mathbb{F}_{17}[x]$ is maximal hence prime

$\mathcal{O}/19\mathcal{O} \cong \mathbb{F}_{19}[x]/(x^2+5) \cong \mathbb{F}_{361} = \mathbb{F}_{19^2} = \mathbb{F}_{19}[\sqrt{-5}] = \{a+b\sqrt{-5} : a,b \in \mathbb{F}_{19}\}$

$19\mathcal{O} = (19) \subset \mathcal{O}$ is maximal i.e. prime

$\mathcal{O}/23\mathcal{O} \cong \mathbb{F}_{23} \oplus \mathbb{F}_{23}$: $(23) \subset \mathcal{O}$ splits as $(23) = \mathfrak{S}\mathfrak{S}'$, $\mathfrak{S} \neq \mathfrak{S}'$ prime ideals in $\mathcal{O}$.

$x^2+5 = (x-15)(x-8)$ in $\mathbb{F}_{23}[x]$

$-2 = 25 = 5^2$

$5 = -18 = -2 \cdot 9 = 5^2 3^2 = 15^2$

$\mathcal{O}/23\mathcal{O} \cong \mathbb{F}_{23}[x]/(x^2+5) = \mathbb{F}_{23}[x]/((x-15)(x-8)) \cong \mathbb{F}_{23}[x]/(x-15) \oplus \mathbb{F}_{23}[x]/(x-8) = \mathbb{F}_{23} \oplus \mathbb{F}_{23}$

Theorem In $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$, $p \in \mathbb{Z}$ ordinary prime, $(p) = p\mathcal{O}$

- ramifies iff $p \in \{2, 5\}$
- splits iff $p \equiv 1, 3, 7$ or $9 \mod 20$
- remain prime iff $p \equiv 11, 13, 17$, or $19 \mod 20$.

To prove this, it suffices to see how x^2+5 factors in $\mathbb{F}_p[x]$.

i.e. whether or not -5 is a square in $\mathbb{F}_p = \{0, 1, 2, \cdots, p-1\}$.

$\left(\frac{-5}{p}\right) = \begin{cases} +1 & \text{if } -5 \text{ is a nonzero square in } \mathbb{F}_p \\ -1 & \text{if } -5 \text{ is a nonsquare in } \mathbb{F}_p \\ 0 & \text{if } -5 = 0 \text{ in } \mathbb{F}_p. \end{cases}$

the Legendre Symbol for odd primes p.

eg. $\left(\frac{-5}{19}\right) = -1$, $\left(\frac{-5}{23}\right) = +1$, $\left(\frac{-5}{5}\right) = 0$

Quadratic Reciprocity: If $p \neq q$ are distinct odd rational primes then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if at least one of } p,q \text{ is } \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \bmod 4. \end{cases}$

If $p \neq 2, 5$ then $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)$

$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4 \end{cases}$

$\underbrace{\left(\frac{5}{p}\right)}_{\pm 1}\underbrace{\left(\frac{p}{5}\right)}_{\pm 1} = 1 \implies \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$

$\mathbb{F}_5 = \{0, \underbrace{1, 2}_{\text{nonsquares}}, \underbrace{3, 4}_{\text{squares}}\}$

eg. $\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = -1$

$\left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1$

$\left(\frac{-5}{23}\right) = \left(\frac{-1}{23}\right)\left(\frac{5}{23}\right) = (-1)(-1) = 1 \implies -5$ is a square in $\mathbb{F}_{23}$ $\quad (15^2 = 8^2 = -5)$

$\left(\frac{-5}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{5}{17}\right) = 1 \cdot (-1) = -1 \implies -5$ is a nonsquare in $\mathbb{F}_{17}$.

$\mathcal{O} \cap \mathbb{Z} = (p) \subset \mathbb{Z}$ (prime)

The nonzero prime ideals in $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$ are

- $\mathfrak{p} = (2, 1+\sqrt{-5})$, $\mathfrak{q} = (3, 1+\sqrt{-5})$ lying above $2, 3 \in \mathbb{Z}$
- $(p) = p\mathcal{O}$, $p \in \mathbb{Z}$ ordinary prime of the form $p = 20k+11$, $20k+13$, $20k+17$, $20k+19$
- prime ideals $\mathfrak{k} \subset \mathcal{O}$ lying above rational primes $p \in \mathbb{Z}$, $p \equiv 1, 3, 7$ or $9 \bmod 20$.
  i.e. $p \in \{7, 11, 13, 17, 19, 31, \cdots\}$

Next: Which primes ramify in an extension?
All primes dividing the discriminant.

The extension $K \supset \mathbb{Q}[\sqrt{-5}]$ (or $\mathbb{Z}[\sqrt{-5}] \supset \mathbb{Z}$) has discriminant -20. We'll talk about this next.

A lattice in $\mathbb{R}^n$ is $\{a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n : a_i \in \mathbb{Z}\}$ where $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of $\mathbb{R}^n$.

For every number field $K \supseteq \mathbb{Q}$ i.e. extension field of degree $n = [K:\mathbb{Q}] < \infty$
K has a basis $\alpha_1, \ldots, \alpha_n$ such that $\mathcal{O} = \{\alpha \in K : \alpha \text{ is an alg. int}\}$ = lattice generated by $\alpha_1, \ldots, \alpha_n$.

eg. $K = \mathbb{Q}[\sqrt{-5}]$ has basis $\{1, \sqrt{-5}\}$
$K = \{a + b\sqrt{-5} : a, b \in \mathbb{Q}\}$
$\mathcal{O} = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ is a lattice in $\mathbb{Q}^2$

The trace map $\mathrm{tr} : K \to \mathbb{Q}$ of the extension is the map $\mathrm{tr}(\alpha) = \alpha + \sigma(\alpha)$ where $\sigma(a+b\sqrt{-5}) = \overline{a+b\sqrt{-5}} = a - b\sqrt{-5}$
$\sigma \in \mathrm{Aut}\, K = \{\iota, \sigma\}$, $\iota(\alpha) = \alpha$

The norm map $N : K \to \mathbb{Q}$ of the extension is
$N(\alpha) = \alpha\,\sigma(\alpha) = \alpha\bar{\alpha}$
$N(\alpha\beta) = N(\alpha)N(\beta)$ $\qquad \mathrm{tr}(\alpha+\beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta)$

The discriminant is the determinant of the $n \times n$ matrix whose (i,j)-entry is $\mathrm{tr}(\alpha_i\alpha_j)$.

For $K = \mathbb{Q}[\sqrt{-5}]$ with basis $\{1, \sqrt{-5}\}$, (α_1, α_2),
$$\mathrm{disc}_{\mathbb{Q}} K = \det \begin{bmatrix} \mathrm{tr}(1\cdot 1) & \mathrm{tr}(1\cdot\sqrt{-5}) \\ \mathrm{tr}(\sqrt{-5}\cdot 1) & \mathrm{tr}(\sqrt{-5}\cdot\sqrt{-5}) \end{bmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & -10 \end{vmatrix} = -20$$

$\mathrm{tr}\, 1 = 1 + 1 = 2$
$\mathrm{tr}\, \sqrt{-5} = \sqrt{-5} + (-\sqrt{-5}) = 0$
$\mathrm{tr}(-5) = -5 + \overline{-5} = -10$

The rational primes dividing -20 are $2, 5$.
These are the ordinary primes that ramify in the extension.

For every nonzero ideal $\mathcal{A} \subseteq \mathcal{O}$ we can think of $\mathcal{A}$ as a sublattice of $\mathcal{O}$ with only finitely many cosets. $|\mathcal{O}/\mathcal{A}|$ = number of cosets = norm of the ideal $\mathcal{A} \subseteq \mathcal{O}$.

$\mathcal{O}/\mathcal{A} = \{v + \mathcal{A} : v \in \mathcal{O}\}$ quotient of additive abelian groups i.e. quotient of $\mathbb{Z}$-modules

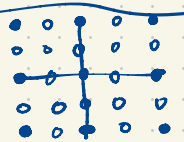
$v + \mathcal{A} = \{v + x : x \in \mathcal{A}\}$

If $\alpha \in \mathcal{O}$ then $(\alpha) = \alpha\mathcal{O} \subseteq \mathcal{O}$ and $N((\alpha)) = |N(\alpha)|$ (absolute value)

$N(\mathcal{AB}) = N(\mathcal{A})N(\mathcal{B})$ $\quad |\mathcal{O}/\mathcal{AB}| = |\mathcal{O}/\mathcal{A}| \cdot |\mathcal{O}/\mathcal{B}|$ This may be obvious if $\mathcal{A}, \mathcal{B}$ rel. prime i.e. $\mathcal{A} + \mathcal{B} = \mathcal{O}$

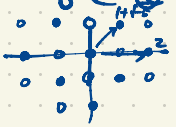
eg. $\mathfrak{p} = (2, 1+\sqrt{5})$ has norm 2

$\mathfrak{p}^2 = (2)$



$\mathcal{O} = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$

$\mathfrak{p} \subset \mathcal{O}$ is generated by 2, $1+\sqrt{5}$ $(2,0)$ $(1,1)$



$\mathfrak{p}$: •

$\mathcal{O}$: ○, • two cosets of $\mathfrak{p}$

$\mathfrak{p} = \{a + b\sqrt{5} : a, b \in \mathbb{Z},\ a+b \text{ even}\}$

$N(\mathfrak{p}) = |\mathcal{O}/\mathfrak{p}| = 2$

$\mathcal{O} = \mathfrak{p} \sqcup (1 + \mathfrak{p})$

To prove $\mathfrak{p}^2 = (2)$ we can argue as before $\mathfrak{p}^2 \subseteq (2)$ and $(2) \subseteq \mathfrak{p}^2$. slightly tricky

Or: $N(\mathfrak{p}^2) = N(\mathfrak{p})^2 = 2^2 = 4$

$N((2)) = |N(2)| = |2 \cdot 2| = 4$

$\mathcal{O}$ has fund. domain $[0,1) \times [0,1)$

$\mathbb{R}^2 = \bigsqcup_{v \in \mathcal{O}} (v + D)$

$\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$ has two kinds of nonzero ideals:

- (principal) $(11), (13), (17), (19), (\sqrt{-5})$, | $(7) = \mathfrak{R}\mathfrak{R}'$, $(2) = \mathfrak{P}^2$, ... $(6) = \mathfrak{P}^2\mathfrak{q}\bar{\mathfrak{q}}$, $(3) = \mathfrak{q}\bar{\mathfrak{q}}$

  ($(\sqrt{-5})$: prime)

- (non-principal) $\mathfrak{P} = (2, 1+\sqrt{-5})$, $\mathfrak{q} = (3, 1+\sqrt{-5})$, $\mathfrak{R}$, ... | $\mathfrak{P}^3 = 2\mathfrak{P}$

  ($\mathfrak{P}, \mathfrak{q}, \mathfrak{R}$: prime; $\mathfrak{P}^3 = 2\mathfrak{P}$: non-prime)

	principal	non-principal
principal	principal	non-principal
non-principal	non-principal	principal

$(a)(b) = (ab)$

is a (multiplicative) group of order 2.

For every number field $K \supseteq \mathbb{Q}$ i.e. finite extension field

we have the ring of integers $\mathcal{O} \supseteq \mathbb{Z}$ in this extension

the nonzero (fractional) ideals of $\mathcal{O}$ form a mult. group and the principal ideals form a subgroup.

The quotient group $\{\text{ideals}\}/\{\text{principal ideals}\}$ (the ideal class group of the extension $K \supseteq \mathbb{Q}$)

The order of this group is denoted $h = h_K = |\{\text{ideals}\}/\{\text{principal ideals}\}|$ is a finite group.

or ideal class number (= number of ideal classes = number of cosets of principal ideals) is the class number of the extension $K \supseteq \mathbb{Q}$.

$h_{\mathbb{Q}[\sqrt{-5}]} = 2$

$h_{\mathbb{Q}} = 1$. (every nonzero ideal in $\mathbb{Z}$ is principal).

$h_{\mathbb{Q}[i]} = 1$

$h_K = 1$ iff $\mathcal{O}$ has unique factorization (i.e. of elements). (ideals always have unique factorization)

Consequence of Minkowski's Theorem

Dedekind zeta function $\zeta_K(s)$ of a number field K.

$N(A) = |\mathcal{O}/A|$

eg. $\zeta_{\mathbb{Q}}(s) = \zeta(s)$ = Riemann zeta function

$s \in \mathbb{C}$, $\zeta_K(s) = \sum_{(0) \neq A \subseteq \mathcal{O}} \frac{1}{N(A)^s}$

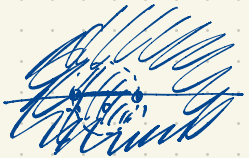
Eg. Every ideal $A \subseteq \mathbb{Z}$ is principal, $A = n\mathbb{Z} = (n)$ for some $n \in \mathbb{Z}$, $(-n) = (n)$

$N((0)) = |\mathbb{Z}/(0)| = |\mathbb{Z}| = \infty$

$N((n)) = |\mathbb{Z}/(n)| = n.$

$\zeta(s) = \zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$ (for $\mathrm{Re}\, s > 1$) $\qquad \zeta(2) = \frac{\pi^2}{6}$

$\zeta(s)$ is analytic on $\mathbb{C} - \{1\}$. (pole at $s=1$)



Compare: $f(s) = 1 + s + s^2 + s^3 + \cdots$, convergent for $|s| < 1$.

This extends to the entire plane $\mathbb{C}$ as a meromorphic function with a simple pole at $s = 1$.

$f(s) = \frac{1}{1-s}$

In number theory we consider Dirichlet series $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, $a_n \in \mathbb{R}$.

If it converges at some point $P \in \mathbb{C}$ then it converges "to the right"

The typical domain of convergence of a Dirichlet series is a half-plane $\mathrm{Re}\, s > s$.

The zeta function $\zeta_K(s)$ of a number field converges in $\mathrm{Re}\, s > 1$. But $\zeta_K(s)$ continues analytically to $\mathbb{C}$ with a single pole at $s=1$.

"Dirichlet series" includes zeta functions and L-functions.

$\zeta(2) = \frac{\pi^2}{6}$ the Basel problem

The Riemann zeta function has an Euler factorization

$$\zeta(s) = \prod_p \frac{1}{1-\frac{1}{p^s}} = \frac{1}{1-\frac{1}{2^s}} \cdot \frac{1}{1-\frac{1}{3^s}} \cdot \frac{1}{1-\frac{1}{5^s}} \cdot \frac{1}{1-\frac{1}{7^s}} \cdot \frac{1}{1-\frac{1}{11^s}} \cdot \frac{1}{1-\frac{1}{13^s}} \times \cdots$$

$$= \left(1+\frac{1}{2^s}+\frac{1}{4^s}+\frac{1}{8^s}+\frac{1}{16^s}+\cdots\right)\left(1+\frac{1}{3^s}+\frac{1}{9^s}+\cdots\right)\left(1+\frac{1}{5^s}+\cdots\right)\left(1+\frac{1}{7^s}+\cdots\right)\left(1+\frac{1}{11^s}+\cdots\right)\left(1+\frac{1}{13^s}+\cdots\right)$$

$$= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s} + \frac{1}{8^s} + \cdots$$

Analytic form of the FTA = fundamental theorem of arithmetic

This works for every number field $K \supseteq \mathbb{Q}$:

$$\zeta_K(s) = \sum_{0 \neq \mathcal{A} \subseteq \mathcal{O}} \frac{1}{N(\mathcal{A})^s} = \prod_{0 \neq \mathfrak{p} \subset \mathcal{O}} \left(\frac{1}{1-\frac{1}{N\mathfrak{p}^s}}\right) = \prod_{\mathfrak{p}} \frac{1}{1-N(\mathfrak{p})^{-s}} = \prod_{\mathfrak{p}} \left(1-N(\mathfrak{p})^{-s}\right)^{-1}$$

since ideals in $\mathcal{O}$ have unique factorization as products of prime ideals

$N(\mathcal{A}) = |\mathcal{O}/\mathcal{A}|$

$\mathcal{A}$ nonzero ideal

nonzero prime ideals $\mathfrak{p} \subset \mathcal{O}$

Eg. $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$ has prime ideals:

Norm 2: $\mathfrak{p} = (2, 1+\sqrt{-5})$

Norm 3: $\mathfrak{q} = (3, 1+\sqrt{-5})$, $\bar{\mathfrak{q}} = (3, 1-\sqrt{-5})$

Norm 5: $(\sqrt{-5})$

Norm 7: $\mathfrak{R}, \mathfrak{R}' = \bar{\mathfrak{R}}$

Norm 11^2: (11) $\quad \mathcal{O}/_{11\mathcal{O}} = \mathcal{O}/_{(11)} \cong \mathbb{F}_{121}$

Norm 31: $\mathfrak{Q}, \bar{\mathfrak{Q}}$ $\quad \mathfrak{Q}\bar{\mathfrak{Q}} = (31)$ $\quad N(\mathfrak{Q}) = |\mathcal{O}/\mathfrak{Q}| = 31$.

$$\zeta_{\mathbb{Q}[\sqrt{-5}]}(s) = \frac{1}{1-\frac{1}{2^s}}\left(\frac{1}{1-\frac{1}{3^s}}\right)^2 \frac{1}{1-\frac{1}{5^s}}\left(\frac{1}{1-\frac{1}{7^s}}\right)^2 \frac{1}{1-\frac{1}{11^{2s}}} \cdot \frac{1}{1-\frac{1}{13^{2s}}} \cdot \frac{1}{1-\frac{1}{17^{2s}}} \frac{1}{1-\frac{1}{19^{2s}}} \cdot \left(\frac{1}{1-\frac{1}{31^s}}\right)^2 \times \cdots$$

Non-prime ideals: $(2) = \mathfrak{p}^2$ of norm 4

$\mathfrak{p}\mathfrak{q} = (1+\sqrt{-5})$ of norm 6

$\mathfrak{p}\bar{\mathfrak{q}} = (1-\sqrt{-5})$ . . . . .

$$\zeta_{\mathbb{Q}[\sqrt{-5}]}(s) = \frac{1}{1-\frac{1}{2^s}}\left(\frac{1}{1-\frac{1}{3^s}}\right)^2 \frac{1}{1-\frac{1}{5^s}}\left(\frac{1}{1-\frac{1}{7^s}}\right)^2 \frac{1}{1-\frac{1}{11^s}} \cdot \frac{1}{1-\frac{1}{13^s}} \cdot \frac{1}{1-\frac{1}{17^s}} \frac{1}{1-\frac{1}{19^s}} \cdot \left(\frac{1}{1-\frac{1}{31^s}}\right)^2 \times \cdots$$

$$= \left(1+\frac{1}{2^s}+\frac{1}{4^s}+\frac{1}{8^s}+\cdots\right)\left(1+\frac{2}{3^s}+\frac{3}{9^s}+\frac{4}{27^s}+\cdots\right)\left(1+\frac{1}{5^s}+\frac{1}{25^s}+\cdots\right)\times\cdots$$

$$= \sum_{0 \neq A \subseteq \mathcal{O}} \frac{1}{N(A)^s}$$

$$= 1 + \frac{1}{2^s} + \frac{2}{3^s} + \cdots$$

Non-prime ideals: $(2) = \mathfrak{q}^2$ of norm 4
$\mathfrak{q}\bar{\mathfrak{q}} = (1+\sqrt{-5})$ of norm 6
$\mathfrak{q}\bar{\mathfrak{q}} = (1-\sqrt{-5})$ . . . . .

↑ 2 ideals of norm 3: $\mathfrak{q}, \bar{\mathfrak{q}}$

But what else can we do with zeta functions?

Eg. If m,n are randomly chosen large integers, what is the probability that m,n are relatively prime? About 61%:

$$\lim_{N\to\infty} \frac{\{(m,n) \in [1,N]^2 : \gcd(m,n) = 1\}}{N^2} = \frac{6}{\pi^2} \approx 0.60793$$

Why? $\gcd(m,n)=1$ $\iff$

- m,n are not both divisible by 2 — with probability $1-\frac{1}{4} = 1-\frac{1}{2^2}$
- and . . . . . 3 — . . . . . $1-\frac{1}{9} = 1-\frac{1}{3^2}$
- . . . . . 5 — . . . . . $1-\frac{1}{25} = 1-\frac{1}{5^2}$
- . . . . . 7 — . . . . . $1-\frac{1}{49} = 1-\frac{1}{7^2}$
- . . . . . 11 — . . . . . $1-\frac{1}{121} = 1-\frac{1}{11^2}$
- and . . . .

with probability $(1-\frac{1}{2^2})(1-\frac{1}{3^2})(1-\frac{1}{5^2})(1-\frac{1}{7^2})(1-\frac{1}{11^2})\times\cdots = \frac{1}{\zeta(2)}$

This value $\frac{1}{\zeta(2)} \approx 0.61$ is also the probability that a randomly chosen large integer n is squarefree. (not divisible by any prime more than once).

Given $m_1, m_2, \cdots, m_k \in \mathbb{Z}$, we say $m_1, \cdots, m_k$ are relatively prime if

$\gcd(m_1, m_2, \cdots, m_k) = 1 \iff (m_1, m_2, \cdots, m_k) = (1) = \mathbb{Z}$

$m_1\mathbb{Z} + m_2\mathbb{Z} + \cdots + m_k\mathbb{Z}$

eg. $6, 10, 15$ are relatively prime since $\gcd(6,10,15) = 1$.

Given three large integers, how often are they relatively prime? $\frac{1}{\zeta(3)}$.

---

eg. $K = \mathbb{Q}[\sqrt{-5}]$, $\mathcal{O} = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$.

Given $\alpha, \beta \in \mathcal{O}$ at random, how often are α, β relatively prime? i.e. $\gcd(\alpha, \beta) = 1$ (the only elements of the ring $\mathcal{O}$ dividing both α, β are the units ± 1).

$\iff (\alpha, \beta) = \mathcal{O} = (1)$

The prob. that $\alpha, \beta \in \mathcal{O}$ are relatively prime is $\frac{1}{\zeta_K(2)}$

$$\zeta_K(s) = \underbrace{\frac{1}{1-\frac{1}{2^s}} \cdot \frac{1}{1-\frac{1}{5^s}}}_{2,5 \text{ ramify}} \cdot \underbrace{\prod_{p \equiv 1,3,7,9 \bmod 20} \left(\frac{1}{1-\frac{1}{p^s}}\right)^2}_{\text{primes that split}} \cdot \underbrace{\prod_{p \equiv 11,13,17,19 \bmod 20} \left(\frac{1}{1-\frac{1}{p^{2s}}}\right)}_{p \text{ remains prime}},$$

$$= \underbrace{\zeta(s)}_{\text{Riemann zeta } \zeta_{\mathbb{Q}}(s)} \cdot \frac{1}{1-\frac{1}{3^s}} \cdot \frac{1}{1-\frac{1}{7^s}} \cdot \frac{1}{1+\frac{1}{11^s}} \cdot \frac{1}{1+\frac{1}{13^s}} \cdot \frac{1}{1+\frac{1}{17^s}} \cdot \frac{1}{1+\frac{1}{19^s}} \cdot \frac{1}{1-\frac{1}{23^s}} \cdot \frac{1}{1-\frac{1}{29^s}} \cdot \frac{1}{1+\frac{1}{31^s}} \cdots$$

$\zeta_K(2) \approx 1.855557$

$\frac{1}{\zeta_K(2)} \approx 0.53892$

About 54% of the time, $\alpha, \beta \in \mathcal{O}$ are relatively prime.

$\mathbb{Q}[\sqrt{5}] \supset \mathbb{Q}$ has as its ring of integers $\mathbb{Z}[\sqrt{5}] = \{a+b\sqrt{5} : a,b \in \mathbb{Z}\}$

$\alpha \in K \supseteq \mathbb{Q}$ is an algebraic integer if

- α is a root of a monic poly in $\mathbb{Z}[x]$
- Equivalently, the min. poly. of α over $\mathbb{Q}$ has integer coefficients

$\mathbb{Q}[\sqrt{5}] \supset \mathbb{Q}$ has as its ring of integers $\mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \{\frac{a+b\sqrt{5}}{2} : a,b \in \mathbb{Z},\ a \equiv b \bmod 2\} = \mathbb{Z}[\sqrt{5}] \sqcup (\frac{1+\sqrt{5}}{2} + \mathbb{Z}[\sqrt{5}])$

Not just $\mathbb{Z}[\sqrt{5}] = \{a+b\sqrt{5} : a,b \in \mathbb{Z}\}$

$\frac{1+\sqrt{5}}{2}$ is a root of $x^2 - x - 1 \in \mathbb{Z}[x]$ monic

How do we find all the algebraic integers in K?

Theorem The ring of integers in $\mathbb{Q}[\sqrt{5}]$ is $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

Proof Let $\mathcal{O} \subset \mathbb{Q}[\sqrt{5}]$ be the ring of alg. int. $\mathcal{O}$ contains 1 (root of $x-1$) and $\sqrt{5}$ (root of x^2-5).

so $\mathcal{O} \supseteq \mathbb{Z}[\sqrt{5}] = \{a+b\sqrt{5} : a,b \in \mathbb{Z}\}$

If $\alpha = a+b\sqrt{5} \in \mathcal{O}$ $(a,b \in \mathbb{Q})$ then $\bar{\alpha} = a-b\sqrt{5} \in \mathcal{O}$ Since conjugation $\alpha \mapsto \bar{\alpha}$ is an automorphism of $\mathbb{Q}$

(If $f(\alpha)=0$ where $f(x) \in \mathbb{Z}[x]$ monic then $f(\bar{\alpha}) = \overline{f(\alpha)} = \bar{0} = 0$ so $\bar{\alpha} \in \mathbb{Q}[\sqrt{5}]$ is also an alg. int.)

$\Rightarrow \alpha + \bar{\alpha} = 2a \in \mathcal{O}$ since $\mathcal{O}$ is a ring. $\Rightarrow 2a \in \mathbb{Z}$, $a^2 - 5b^2 \in \mathbb{Z}$ $\Rightarrow$ (elementary) $\alpha \in \{$ a,b both integers or both integers $+\frac{1}{2}$.

$\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$

If $r \in \mathbb{Q}$, its min. poly. over $\mathbb{Q}$ is $x - r \in \mathbb{Z}[x] \Rightarrow r \in \mathbb{Z}$.

Similarly the integers in $\mathbb{Q}[\sqrt{-5}]$ are just $\mathbb{Z}[\sqrt{-5}]$.

Generalization to quadratic number fields (degree 2 extensions $K > \mathbb{Q}$, $[K:\mathbb{Q}] = 2$).

Theorem The quadratic number fields are the fields of the form $\mathbb{Q}[\sqrt{d}]$, $d \neq 1, 0$, d squarefree, $d \equiv 1, 2$ or $3 \bmod 4$.

(Squarefree: not divisible by p^2 for any prime p).

$\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[\sqrt{2}]$

The real quadratic fields $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{6}]$, $\mathbb{Q}[\sqrt{7}]$, $\mathbb{Q}[\sqrt{10}]$, $\mathbb{Q}[\sqrt{11}]$, $\mathbb{Q}[\sqrt{13}]$, ...

The imaginary quadratic fields are $\mathbb{Q}[\sqrt{-1}] = \mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{-2}]$, $\mathbb{Q}[\sqrt{-3}]$, $\mathbb{Q}[\sqrt{-5}]$, $\mathbb{Q}[\sqrt{-6}]$, ...

Proof Let K be a quadratic field. It has a basis $\{1, \alpha\}$. α^2 is a $\mathbb{Q}$-lin. comb. of $1, \alpha \Rightarrow \alpha$ is a root of $x^2 + bx + c \in \mathbb{Q}[x]$. $\Rightarrow \alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2} = \frac{-b \pm \sqrt{D}}{2}$, $D \in \mathbb{Q}$. $K = \mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{d}]$

$D = r^2 \cdot d$ $r \in \mathbb{Q}$, $d \in \mathbb{Z}$. squarefree.

Theorem If $d \equiv 2$ or $3 \bmod 4$ then the alg. int. in $K = \mathbb{Q}[\sqrt{d}]$ are just $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$

If $d \equiv 1 \bmod 4$ then the alg. int. in $K = \mathbb{Q}[\sqrt{d}]$ are $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{\frac{a + b\sqrt{d}}{2} : a, b \in \mathbb{Z} \text{ of the same parity}\right\}$

eg. $\mathbb{Q}[\sqrt{-3}] = \mathbb{Q}[\omega]$ has ring of integers $\mathbb{Z}[\omega]$, $\omega = \frac{-1+\sqrt{-3}}{2} = e^{2\pi i/3}$ since $-3 \equiv 1 \bmod 4$.

$\mathbb{Q}[i]$ - - - - - - $\mathbb{Z}[i]$

$\mathbb{Z}[\omega]$: Eisenstein integers

$\mathbb{Z}[i]$: Gaussian integers

$\mathbb{Z}$, $\mathbb{Z}[\sqrt{5}]$, $\mathbb{Z}[\sqrt{-5}]$: roots of unity ± 1 only.

$\mathbb{Z}[i]$: units $\pm 1, \pm i$

$\mathbb{Z}[\omega]$: units $\pm 1, \pm\omega, \pm\bar{\omega} = \pm\omega^2$.