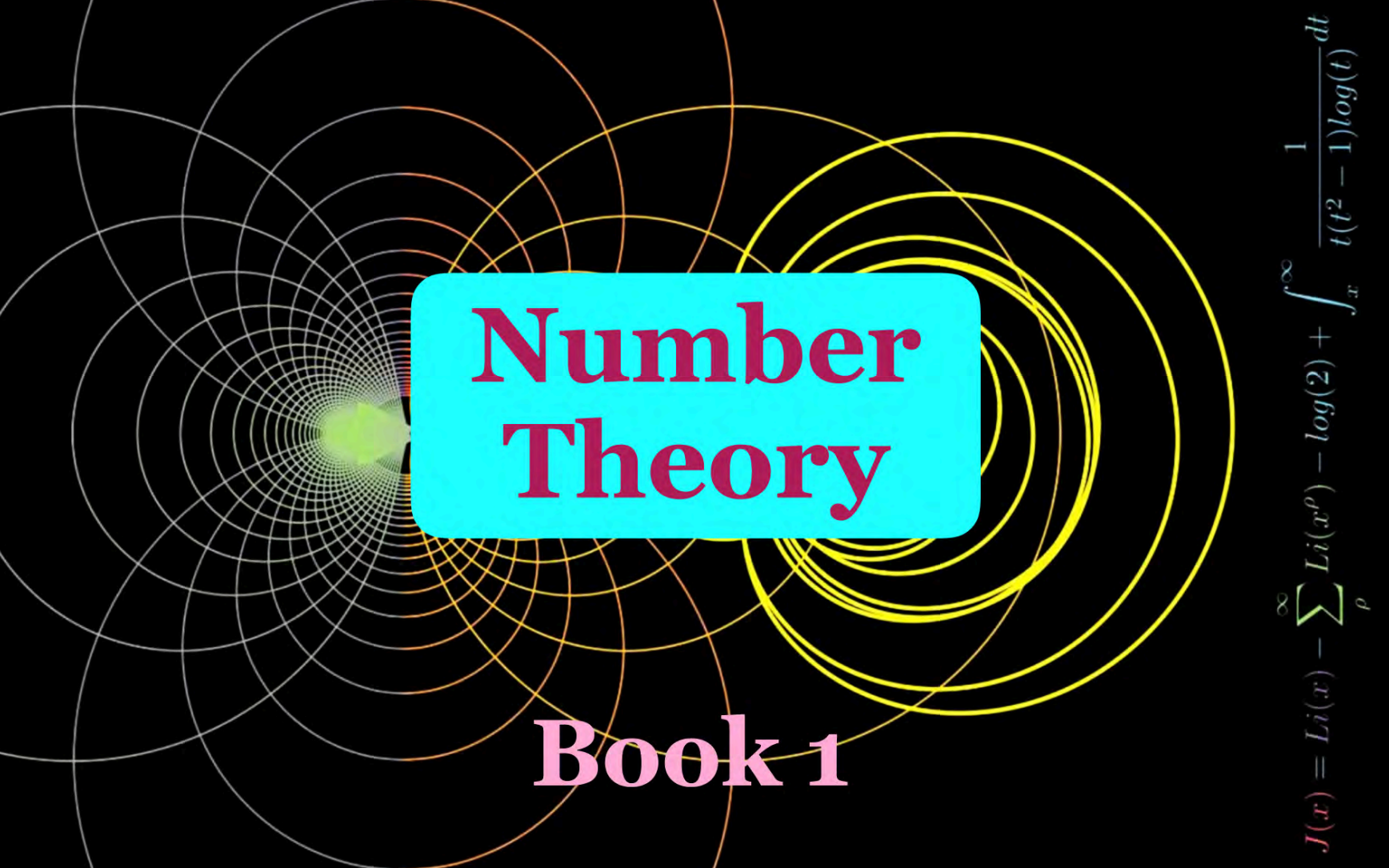

Number
Theory
Book 1
$J(x) = Li(x) - \sum_{\rho} Li(x^{\rho}) - \log(2) + \int_x^{\infty} \frac{1}{t(t^2-1)\log(t)} dt$

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
$\vdots$	$\vdots$

$x^2 - 5y^2 = 1 \iff (x + y\sqrt{5})(x - y\sqrt{5}) = 1$ 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 $\mathbb{Q}$.

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

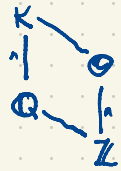
$[\mathbb{C}:\mathbb{R}] = 2$

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

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

$K \supseteq \mathbb{Q}$ 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 $\mathcal{O} \supseteq \mathbb{Z}$

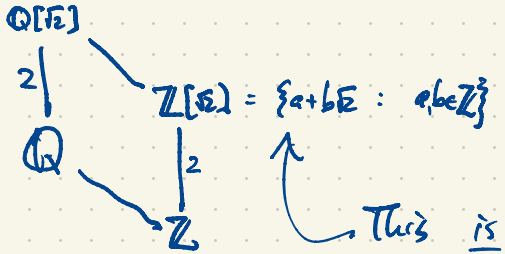
$\alpha_1, \dots, \alpha_n$ basis for $K \supseteq \mathbb{Q}$

$\mathcal{O}$ 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

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

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

$\mathbb{Q} \quad \mid$

$\mathbb{Z}$

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

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

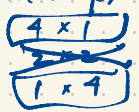
$a^2 + 5b^2 \Rightarrow (a, b) = (\pm 1, 0) \Rightarrow \alpha = \pm 1$.

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

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

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

$\mathbb{Q}$ — $\mathbb{Z}$ (index 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.