

field	rational numbers \mathbb{Q}	Gaussian number field $\mathbb{Q}(i)$	quadratic number field $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ squarefree, $d \neq 0, 1$	general number field K $n := [K : \mathbb{Q}] < \infty$
ring of integers	\mathbb{Z}	$\mathbb{Z}[i]$	$\mathbb{Z}[\sqrt{d}]$	\mathcal{O}_K
\mathbb{Z} -basis	$\mathbb{Z} \cdot 1$	$\mathbb{Z} \cdot 1 + \mathbb{Z} \cdot i$	$\mathbb{Z} + \mathbb{Z}\sqrt{d}$ if $d \equiv 1 \pmod{4}$	\exists integral basis, i.e., $\mathcal{O}_K = \mathbb{Z}\omega_1 + \dots + \mathbb{Z}\omega_n$ for some $\omega_1, \dots, \omega_n \in \mathcal{O}_K$
multi.licative structure	unique prime factorization	unique prime factorization $p \equiv 3 \pmod{4}$ stay prime $p \equiv 1 \pmod{4}$ split into primes (e.g. $5 = 2^2 + 1^2 = (2+i)(2-i)$ $2 = -i(1+i)^2$)	unique prime factorization $d < 0$: for $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$ $d > 0$: for $d \in \{2, 3, 5, 6, 7, 11, 13, \dots\}$ For all other d there is just a unique factorization of ideals into prime ideals	in general only unique factorization of ideals into prime ideals
invertible elements (group of units)	± 1 $(\cong \mathbb{Z}/2\mathbb{Z})$	$\pm 1, \pm i$ $(\cong \mathbb{Z}/4\mathbb{Z})$	$\pm 1, \pm i$ if $d = -1$ ($\cong \mathbb{Z}/4\mathbb{Z}$) $\pm 1, \frac{\pm 1 \pm i\sqrt{d}}{2}$ if $d \equiv -3 \pmod{4}$ ($\cong \mathbb{Z}/6\mathbb{Z}$) ± 1 ($\cong \mathbb{Z}/2\mathbb{Z}$) for all other $d < 0$ $\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ for all $d > 0$ (e.g., $\pm(1 + \sqrt{2})^n$, $n \in \mathbb{Z}$ if $d = 2$)	Dixmier's unit theorem

Applications to Diophantine equations, e.g. $x^2 + 1 = y^3$ has only $(x, y) = (0, 1)$, as a solution in \mathbb{Z}^2 . (Basic idea: $y^3 = x^2 + 1 = (x+i)(x-i)$. Use the arithmetic structure of $\mathbb{Z}[i]$ to deduce: $\exists \alpha, \beta \in \mathbb{Z} : x+i = (\alpha+i\beta)^3 = \alpha^3 - 3\alpha\beta^2 + i(3\alpha^2\beta - \beta^3)$. Solve the system $\begin{cases} \alpha^3 - 3\alpha\beta^2 = x \\ 3\alpha^2\beta - \beta^3 = 1 \end{cases}$)

Applications to Fermat's Last Theorem: $z^n = x^{n-1}y^n = (x+y)(x+iy)\dots(x+i^{n-1}y)$ with $z = e^{2\pi i/n}$. Work in the ring $\mathbb{Z}[\zeta]$ of the cyclotomic field $\mathbb{Q}(\zeta)$. (One can prove Fermat's Last Theorem in this way only if $\mathbb{Z}[\zeta]$ is a unique factorization domain.)