Dedekind introduced the term "ideal" in analogy with the ideal object Kummer adjoined to cyclotomic fields.... Thus for Dedekind new objects should be constructed as sets of known objects rather than by adding new symbols satisfying special conditions (as, for example, Kummer did with his ideal objects).
Jay R. Goldman, The Queen of Mathematics. 1998. p. 266

$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ Polynom

$p(\alpha) = 0 \ (a_i \in \mathbb{Q})$ α algebraische Zahl *algebraic number*

$p(\alpha) = 0 \ (a_i \in \mathbb{Z})$ α ganze algebraische Zahl *algebraic integer*

$\mathbb{Q}_d = \mathbb{Q}(\sqrt{d}) = \mathbb{Q} + \sqrt{d}\mathbb{Q}$ quadratischer Zahlkörper *quadratic field*

$\mathbb{Z} + i\mathbb{Z} \subset \mathbb{Q}(\sqrt{-1}) \subset \mathbb{C}$ Gaußsche ganze Zahlen *Gaussian integers*

$N(q+r\sqrt{d}) := (q+r\sqrt{d})(q-r\sqrt{d}) = q^2 - r^2 d$ Norm in $\mathbb{Q}_d$

$\mathbb{I}_d := \{\alpha \in \mathbb{Q}_d \mid N(\alpha) \in \mathbb{Z}\}$ ganze Zahlen in $\mathbb{Q}_d$

$N(\alpha) = \pm 1$ Einheiten in $\mathbb{I}_d$

($oBdA.$ d quadratfrei)

$x^2 - y^2 d = n$ Pellsche Gleichung

$\mathbb{I}_d = \mathbb{Z}(\sqrt{d}) = \mathbb{Z} + \sqrt{d}\mathbb{Z}$ $d \equiv 2, 3 \mod 4$

$\mathbb{I}_d = \frac{1}{2}\mathbb{Z}(\sqrt{d}) = \frac{1}{2}\mathbb{Z} + \frac{1}{2}\sqrt{d}\mathbb{Z}$ $d \equiv 1 \mod 4$

Euklidischer Algorithmus in $\mathbb{I}_d$ *(bezüglich der Norm)*

Division mit Rest **falls** $\exists \gamma, \delta$

$\alpha, \beta \in \mathbb{I}_d \ \Rightarrow \quad \alpha = \beta\gamma + \delta, \ N(\delta) < N(\beta)$

Euklidischer Ring $:\Leftrightarrow$ Division für alle α, β *Euclidean domain*

Hauptidealring $:\Leftrightarrow$ jedes Ideal Hauptideal *principal ideal ring*

ZPE-Ring (eindeutige Primzahlzerlegung)

unique factorization domain (UFD)

auch: faktorieller Ring *factorial ring*

$:\Leftrightarrow$ eindeutige Zerlegung in irreduzible Elemente

euklidisch $\Rightarrow$ Hauptidealring $\Rightarrow$ faktoriell

$\mathbb{I}_d$ euklidisch $\Leftrightarrow \quad d = -1, -2, -3, -7, -11$

$d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 47, 57, 73$

(Koeffizientenring R) $(a_0, a_1, \cdots, a_n) \in R^{n+1}$

Polynom a $= a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$

Summe $a + b$ $:= (a_i + b_i)$

$:= (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0)$

Produkt $ab := c$ *mit* $c_i = \sum_{j=0}^{i} a_j b_{i-j}$ *(Faltung)*

$:= (a_n b_m)x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m)x^{n+m-1} +$

$\cdots + (a_1 b_0 + a_0 b_1)x + a_0 b_0$

formale Potenzreihe $\sum_{i=0}^{\infty} a_i x^i$ $(a_i) \in R^{\infty}$

Polynom $\Leftrightarrow$ $a_i = 0$ für fast alle i

Polynomring $R[x]$ über R $(R[x], +, \cdot)$

grad $a := \max\{i \mid a_i \neq 0\}$ grad $0 := -\infty$

grad $(a + b) \leq \max\{\text{grad } a, \text{grad } b\}$ grad $ab \leq$ grad $a +$ grad b

R nullteilerfrei $\Rightarrow$ grad $ab =$ grad $a +$ grad b

a Einheiten in $R[x]$ $\Leftrightarrow$ $a = e,\ e \in R^*$ *(konstantes Polynom)*

Polynomfunktion *(zu)* a *(„Evaluation“)*

$f(a) : R \to R,\ r \mapsto a(r) := \sum_i a_i r^i$

Ring $R(x)$ der Polynomfunktionen *(über R)* $(R(x), +, \cdot)$

Ring-Homomorphismus $\varphi : R[x] \to R(x),\ a \mapsto f(a)$

Polynome über $\mathbb{R}$ $\mathbb{R}[x] \cong \mathbb{R}(x)$

$\mathbb{Z}_p(x)$: $x^p - x = 0$ $\Leftarrow x^p \equiv x \bmod p$ *(„Kleiner Fermat“ 1601–65)*

$\Leftarrow r^{\varphi(m)} \equiv 1(m)$ *(Euler 1707–83)* $\Leftarrow g^{|G|} = e$ *(Lagrange 1736–1813)*

(Wilson) $(p-1)! \equiv -1 \bmod p \Leftrightarrow p/((p-1)! + 1)$ $\leftrightarrow$ p prim

---

R Körper $\Rightarrow$ $R[x]$ euklidisch *(bezogen auf* grad a*)*

(Division mit Rest) *(eindeutig)*

$a, b \in R[x] \Rightarrow \exists q, r$ $a = bq + r$ grad $r <$ grad b

$\Rightarrow$ ggT, eindeutige Zerlegung in irreduzible Polynome

$a(r) = 0 \Rightarrow a = (x - r)a'$ *(r ist Nullstelle)*

$\Rightarrow$ Eine Polynomfunktion a hat höchstens grad a Nullstellen.

Fundamentalsatz der Algebra *(Gauß)*

Jedes Polynom über $\mathbb{C}$ zerfällt in Linearfaktoren.