Wichtige Isomorphismen von Ringen

$$R/(0) \cong R \tag{1}$$
$$R/(1) \cong 0 \text{ (Nullring)} \tag{2}$$
$$R/(x,y) \cong (R/(x))\,/\,([y]) \tag{3}$$
$$(R/\mathfrak{a})[X] \cong R[X]\,/\,\mathfrak{a}[X] \tag{4}$$
$$R[X]/(X-a) \cong R \tag{5}$$

Ist außerdem $L \supseteq K$ eine Körpererweiterung und $u \in L$ ein über K algebraisches Element mit Minimalpolynom $m \in K[X]$, so gilt:

$$K(u) = K[u] \cong K[X]/(m) \tag{6}$$

Schließlich gibt es noch den chinesischen Restsatz: Sind $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale mit $\mathfrak{a} + \mathfrak{b} = (1)$, so gilt $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$ und

$$R/(\mathfrak{a}\mathfrak{b}) \cong R/\mathfrak{a} \times R/\mathfrak{b} \tag{7}$$

Anwendung: Primalitäts- und Maximalitätsuntersuchung

Diese Rechenregeln sind in Kombination mit dem Satz

> Ein Ideal $\mathfrak{a}$ eines Rings R ist genau dann ein Primideal (bzw. ein maximales Ideal), wenn der Faktorring $R/\mathfrak{a}$ ein Integritätsbereich (bzw. ein Körper) ist.

nützlich, um ein gegebenes Ideal auf Primalität und Maximalität zu untersuchen.

Beispiele

- Das Ideal $(5, X-3) \subseteq \mathbb{Z}[X]$ ist maximal, denn
  $$\mathbb{Z}[X]/(5, X-3) \overset{(3)}{\cong} (\mathbb{Z}/(5))[X]\,/\,(X-[3]) \overset{(5)}{\cong} \mathbb{Z}/(5)$$
  ist ein Körper.
- Das Ideal $(X^2, X-3) \subseteq \mathbb{Z}[X]$ ist weder prim noch maximal, denn
  $$\mathbb{Z}[X]/(X^2, X-3) \;=\; \mathbb{Z}[X]/(3^2, X-3) \overset{(3)}{\cong} (\mathbb{Z}/(9))[X]\,/\,(X-[3]) \overset{(5)}{\cong} \mathbb{Z}/(9)$$
  ist weder ein Integritätsbereich noch ein Körper.
- Das Ideal $(X^2+1) \subseteq \mathbb{R}[X]$ ist maximal, denn
  $$\mathbb{R}[X]/(X^2+1) \overset{(6)}{\cong} \mathbb{R}(i) = \mathbb{C}$$
  ist ein Körper (von rechts nach links lesen!).
- Das Ideal $(X^2-1) = (X+1)\cdot(X-1) \subseteq \mathbb{R}[X]$ ist weder maximal noch prim, denn
  $$\mathbb{R}[X]/(X^2-1) \overset{(7)}{\cong} \mathbb{R}[X]/(X+1) \times \mathbb{R}[X]/(X-1) \overset{(5)}{\cong} \mathbb{R} \times \mathbb{R}$$
  ist weder ein Integritätsbereich noch ein Körper. Der chinesische Restsatz (7) war anwendbar, denn $(X+1)+(X-1) = (\mathrm{ggT}(X+1, X-1)) = (1)$.

Anwendung: Invertieren in einfachen Körpererweiterungen

Sei $L \supseteq K$ eine Körpererweiterung und $u \in L$ ein über K algebraisches Element mit Minimalpolynom $m \in K[X]$. Dann gilt also $K(u) = K[u] \cong K[X]/(m)$. Somit übertragen sich die Techniken, um in $K[X]/(m)$ Inverse anzugeben, auf $K(u)$.

Sei zur Illustration $x \in K(u)$, dann gibt es ein Polynom $f \in K[X]$ mit $x = f(u)$. Sei $d = af + bm$ mit $a, b \in K[X]$ eine Bézoutdarstellung des größten gemeinsamen Teilers $d := \mathrm{ggT}(f, m)$.

Dann tritt genau einer der folgenden Fälle ein:

- Der größte gemeinsame Teiler d ist ein konstantes Polynom. Dann ist x in $K(u)$ invertierbar mit Inversem $a(u)/d \in K(u)$.
- Der größte gemeinsame Teiler d hat mindestens Grad 1. Dann ist $x = 0$.

Beispiele

- Sei $u := \sqrt{2} \in \mathbb{C}$. Dann hat u das Minimalpolynom $m := X^2 - 2 \in \mathbb{Q}[X]$ über $\mathbb{Q}$ und eine $\mathbb{Q}$-Basis von $\mathbb{Q}(u)$ ist $1, u$.

  Sei $x := 3\sqrt{2} - 5 \in \mathbb{Q}(u)$. Dann können wir obige Überlegung verwenden, um das Inverse x^{-1} als Linearkombination dieser Basis zu schreiben: In der obigen Notation ist $f := 3X - 5$. Eine Nebenrechnung zeigt, dass ein größter gemeinsamer Teiler von f und m das konstante Einspolynom ist, mit Bézoutdarstellung

  $$1 = \left(-\frac{5}{7} - \frac{3}{7}X\right) f + \frac{9}{7} m.$$

  Also lässt sich das Inverse von $x = f(u)$ als

  $$x^{-1} = -\frac{5}{7} - \frac{3}{7}u$$

  schreiben.
- In Blatt 10, Aufgabe 1(d) geht es um ein komplizierteres Beispiel.