KAPITEL 1

Einführung und Wiederholung

Das Kapitel muss noch gründlich überarbeitet werden.

Die Körpertheorie-Vorlesung ist eine Fortsetzung der Algebra-Vorlesung. Wichtige Ergebnisse finden sich in meinem Skript zur Algebra-Vorlesung.

1. Definition und Beispiele

DEFINITION. *Ein* **Körper** *ist ein kommutativer Ring K, für den gilt*

$$K^* = K \setminus \{0\}.$$

Anders ausgedrückt: In K gilt $1 \neq 0$, die Multiplikation ist kommutativ und jedes von 0 verschiedene Element ist invertierbar.

Beispiele:

(1) Die rationalen, reellen und komplexen Zahlen bilden einen Körper: $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$.
(2) Die ganzen Zahlen bilden keinen Körper, da beispielsweise 2 nicht invertierbar ist. (Es ist $\mathbb{Z}^* = \{\pm 1\}$.)
(3) Der Nullring $R = \{0\}$ mit $1 = 0$ bildet keinen Körper, da hier $R^* = R$ gilt.

Bemerkung: Für einen Ring R definiert man für $n \in \mathbb{Z}$ und $a \in R$ das „Produkt“ $n \cdot a$ durch

$$n \cdot a = \begin{cases} \sum_{i=1}^{n} a & \text{für } n \geq 1, \\ 0 & \text{für } n = 0, \\ -\sum_{i=1}^{|n|} a & \text{für } n \leq -1. \end{cases}$$

Für $m, n \in \mathbb{Z}$ und $a \in R$ gilt dann

$$(m+n) \cdot a = m \cdot a + n \cdot a \quad \text{und} \quad (mn) \cdot a = m \cdot (n \cdot a).$$

Für $n \in \mathbb{Z}$ und $1 = 1_R \in R$ schreibt man statt $n \cdot 1_R = n \cdot 1$ auch kurz einfach n; dabei muss natürlich klar sein, in welchem Ring man sich befindet.

Erinnerung an die Division mit Rest in $\mathbb{Z}$: Für $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ kann man eindeutig zerlegen

$$a = qn + r \text{ mit } q, r \in \mathbb{Z} \text{ und } 0 \leq r \leq n-1.$$

Es ist

$$q = \left\lfloor \frac{a}{n} \right\rfloor \text{ und } r = a - \left\lfloor \frac{a}{n} \right\rfloor n.$$

Den Rest r der Division von a durch n schreibt man auch als $a \bmod n$:

$$a \bmod n = r.$$

Damit kann man leicht endliche kommutative Ringe konstruieren: Als zugrundeliegende Menge wählt man

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\},$$

als Addition

$$(a, b) \mapsto (a + b) \bmod n,$$

Datei: kt_einf.tex. Version vom 22.4.2024

und als Multiplikation

$$(a, b) \mapsto (ab) \bmod n.$$

Die Addition schreiben wir als $+$, die Multiplikation als $\cdot$. Die Einheitengruppe ist

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \mathrm{ggT}(n, a) = 1\} \quad \text{mit} \quad |\mathbb{Z}_n^*| = \varphi(n).$$

Ist $a \in \mathbb{Z}_n^*$, so findet man mit dem erweiterten euklidischen Algorithmus $u, v \in \mathbb{Z}$ mit

$$un + va = 1.$$

Dann gilt

$$a^{-1} = v \text{ in } \mathbb{Z}_n.$$

(Mit obiger Konvention wird $k \in \mathbb{Z}$ in $\mathbb{Z}_n$ zu $k \bmod n$. Insbesondere ist $-1 = n - 1$.)
Ist p eine Primzahl, so gilt $\mathbb{Z}_p^* = \{1, \ldots, p-1\} = \mathbb{Z}_p \setminus \{0\}$, $\mathbb{Z}_p$ ist also ein Körper.

DEFINITION. *Für eine Primzahl p wird der Körper $\mathbb{Z}_p$ auch als $\mathbb{F}_p$ geschrieben. Dabei kommt $\mathbb{F}_p$ vom Englischen „finite field". Man findet auch die Schreibweise* $\mathrm{GF}(p)$*, wobei GF für „galois field" steht.*

Bemerkung: Ist R ein Integritätsring, also ein kommutativer Ring mit $1 \neq 0$, sodass für alle $x, y \in R$ die Implikation

$$xy = 0 \quad \Longrightarrow \quad x = 0 \text{ oder } y = 0$$

gilt, so kann man dazu den **Quotientenkörper** bilden:

$$\mathrm{Quot}(R) = \{\frac{a}{b} : a \in R, b \in R \setminus \{0\}\}.$$

Dabei gelten die üblichen Rechenregeln:

- $\frac{a}{b} = \frac{c}{d} \iff ad = bc$.
- $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.
- $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.
- $0 = \frac{0}{1}$, $1 = \frac{1}{1}$.
- $(\frac{a}{b})^{-1} = \frac{b}{a}$ für $a, b \neq 0$.

Beispiel: Ist K ein Körper, $K[x]$ der Polynomring in der Unbestimmten x mit Koeffizienten aus K, so schreibt man den Quotientenkörper von $K[x]$ auch als $K(x)$:

$$K(x) = \{\frac{f(x)}{g(x)} : f(x), g(x) \in K[x], g(x) \neq 0\}.$$

SATZ. *Ist K ein Körper und U eine endliche Untergruppe der multiplikativen Gruppe K^*, so ist U zyklisch, d.h. es gibt ein $g \in K \setminus \{0\}$ mit $U = \langle g \rangle = \{1, g, g^2, \ldots, g^{\mathrm{ord}\,(g)-1}\}$.*

Erinnerung an den Beweis: Sei d ein beliebiger Teiler der Gruppenordnung $|U|$ und

$$U_d = \{x \in K^* : x^d = 1\}.$$

Da die Elemente von U_d die Nullstellen des Polynoms $x^d - 1 \in K[x]$ sind, ein Polynom vom Grad d aber höchstens d Nullstellen hat, gilt $|U_d| \leq d$. Nach einem Satz aus der Gruppentheorie ist damit U eine zyklische Gruppe. ■

FOLGERUNG. *Ist p eine Primzahl, so ist die multiplikative Gruppe $\mathbb{Z}_p^*$ des Körpers $\mathbb{Z}_p$ zyklisch. (Ein erzeugendes Element der Gruppe wird auch* **Primitivwurzel modulo** *p genannt.)*

Beispiel: Wir betrachten $\mathbb{Z}_7^*$. Es gilt (in $\mathbb{Z}_7$)

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 1,$$

also hat 2 die Ordnung 3 und ist kein Erzeuger von $\mathbb{Z}_7^*$.

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1.$$

Also erzeugt 3 die Gruppe $\mathbb{Z}_7^*$. (Daher ist 3 eine Primitivwurzel modulo 7.)

2. Unterkörper, Teikörper, Oberkörper, Körpererweiterungen

Erinnerung: Ist R ein Ring, so nennt man eine Teilmenge $S \subseteq R$ einen **Unterring** von R, falls S mit der Addition und der Multiplikation von R einen Ring bildet und die Eins von R in S enthalten ist. (Man nennt dann R auch einen **Oberring** von S.) Für einen Ring R ist eine Teilmenge $S \subseteq R$ genau dann ein Unterring von R, wenn folgende Bedingungen erfüllt sind:

(1) $0 \in S$,
(2) $x, y \in S \Longrightarrow x + y \in S$,
(3) $x \in S \Longrightarrow -x \in S$,
(4) $1 \in S$,
(5) $x, y \in S \Longrightarrow xy \in S$.

(Dann ist S selbst ein Ring.)

Definition. *Seien K und L Körper mit $K \subseteq L$, sodass K ein Unterring von L ist.*

- *Dann nennt man K einen* **Unterkörper** *oder* **Teilkörper** *von L.*
- *Man nennt L einen* **Oberkörper** *von K.*
- *Das Paar $K \subseteq L$ nennt man dann auch eine* **Körpererweiterung** *und schreibt $L|K$.*
- *Ein* **Zwischenkörper** *M der Körpererweiterung $L|K$ ist ein Unterkörper von L, der auch Oberkörper von K ist: $K \subseteq M \subseteq L$.*

Das folgende Lemma erweitert das Unterring-Kriterium auf Unterkörper.

Lemma (Kriterium für einen Unterkörper). *Sei L ein Körper. Eine Teilmenge $K \subseteq L$ ist genau dann ein Teilkörper von L, wenn folgende Bedingungen erfüllt sind:*

(1) $0 \in K$,
(2) $x, y \in K \Longrightarrow x + y \in K$,
(3) $x \in K \Longrightarrow -x \in K$,
(4) $1 \in K$,
(5) $x, y \in K \Longrightarrow xy \in K$,
(6) $x \in K \setminus \{0\} \Longrightarrow \frac{1}{x} \in K$.

Beispiele: $\mathbb{Q}$ ist ein Teilkörper von $\mathbb{R}$, $\mathbb{R}$ ist ein Teilkörper von $\mathbb{C}$.

Lemma. *Sei K ein Körper.*

(1) *Ist K_i, $i \in I$, eine Familie von Unterkörpern von K, so ist auch der Durchschnitt*

$$\bigcap_{i \in I} K_i$$

ein Unterkörper von K.

(2) *Ist $A \subseteq K$ eine beliebige Teilmenge von L, so ist*

$$\bigcap_{\substack{L \text{ Unterkörper von } K \\ A \subseteq L}} L$$

der kleinste Unterkörper von K, der A enthält.

(Man nennt ihn auch den von A **erzeugten Unterkörper** *von K.)*

Definition. *Sei L ein Oberkörper von K.*

(1) *Ist A eine Teilmenge von L, so schreibt man $K(A)$ für den kleinsten Unterkörper von L, der K und A enthält. ($K(A)$ ist also ein Zwischenkörper der Körpererweiterung $L|K$.)*

(2) *Ist* $A = \{\alpha_1, \ldots, \alpha_n\}$*, so schreibt man statt* $K(\{\alpha_1, \ldots, \alpha_n\})$ *auch kurz*

$$K(\alpha_1, \ldots, \alpha_n).$$

Man sagt, $K(\alpha_1, \ldots, \alpha_n)$ *entsteht aus* K *durch* **Adjunktion** *von* $\alpha_1, \ldots, \alpha_n$*. Für* $K(\alpha_1, \ldots, \alpha_n)$ *sagt man auch „*K **adjungiert** $\alpha_1, \ldots, \alpha_n$*“.*

Bemerkung: Ist $L|K$ eine Körpererweiterung und $\alpha \in L$, so ist - nach Definition - $K[\alpha]$ der kleinste Unterring von L, der K und α enthält. Es gilt also

$$K[\alpha] \subseteq K(\alpha).$$

Man kann genau charakterisieren, wann hier Gleichheit gilt.

Beispiel: Was ist $\mathbb{Q}(i) \subseteq \mathbb{C}$? Wir zeigen, dass

$$\{a + bi : a, b \in \mathbb{Q}\}$$

bereits ein Unterkörper von $\mathbb{C}$ ist. Ist $a + bi \neq 0$, so ist

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i.$$

Die restlichen Eigenschaften des Unterkörperkriteriums sind noch leichter zu überprüfen. Daher gilt

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}.$$

LEMMA. *Ist* L *ein Oberkörper von* K *und* $\alpha \in L$*, so ist*

$$K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_m\alpha^m \in L : m \in \mathbb{N}, a_0, \ldots, a_m \in K\}$$

und

$$K(\alpha) = \{\frac{a_0 + a_1\alpha + \ldots a_m\alpha^m}{b_0 + b_1\alpha + \cdots + b_n\alpha^n} \in L : n, m \in \mathbb{N}, a_0, \ldots, a_m, b_0, \ldots, b_n \in K, b_0 + b_1\alpha + \cdots + b_n\alpha^n \neq 0\}.$$

3. Algebraische und transzendente Elemente

DEFINITION. *Sei* $K \subseteq L$ *eine Körpererweiterung. Ein* $\alpha \in L$ *heißt* **algebraisch über** K*, wenn* $a_0, a_1, \ldots, a_n \in K$ *existieren mit*

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0 \text{ und } \quad (a_0, a_1, \ldots, a_n) \neq (0, 0, \ldots, 0).$$

Andernfalls heißt α **transzendent über** K*.*

Beispiele:

(1) Natürlich ist jedes $\alpha \in K$ algebraisch über K, denn es genügt der Gleichung $\alpha - \alpha = 0$.

(2) Die komplexen Zahlen $\sqrt{2}$, i und $e^{\frac{2\pi i}{5}}$ sind algebraisch über $\mathbb{Q}$, denn

$$(\sqrt{2})^2 - 2 = 0, \quad i^2 + 1 = 0, \quad (e^{\frac{2\pi i}{5}})^5 - 1 = 0.$$

(3) Für die reelle Zahl

$$\alpha = \sqrt[3]{\sqrt{7} - 1}$$

gilt

$$\alpha^3 = \sqrt{7} - 1, \quad \text{also} \quad \alpha^3 + 1 = \sqrt{7}, \quad \text{also} \quad (\alpha^3 + 1)^2 = 7,$$

und somit

$$0 = (\alpha^3 + 1)^2 - 7 = \alpha^6 + 2\alpha^3 + 1 - 7 = \alpha^6 + 2\alpha^3 - 6.$$

Daher ist α algebraisch über $\mathbb{Q}$.

SATZ (Hermite-Lindemann). *Ist* $\alpha \in \mathbb{C} \setminus \{0\}$ *algebraisch über* $\mathbb{Q}$*, so ist* e^α *transzendent über* $\mathbb{Q}$*.*

FOLGERUNG. *Die Zahlen* e *und* π *sind transzendent über* $\mathbb{Q}$*.*

Beweis: Da 1 natürlich algebraisch über $\mathbb{Q}$ ist, ist $e = e^1$ nach Hermite-Lindemann transzendet über $\mathbb{Q}$. Wäre π algebraisch über $\mathbb{Q}$, so auch $2\pi i$. (Dies folgt später aus der allgemeinen Theorie, da auch $2i$ algebraisch über $\mathbb{Q}$ ist.) Also wäre nach Hermite-Lindeman $1 = e^{2\pi i}$ transzendent über $\mathbb{Q}$, was natürlich nicht der Fall ist. ■

SATZ. *Sei $L|K$ eine Körpererweiterung und $\alpha \in L$. Durch Einsetzen $x = \alpha$ erhalten wir einen Ringhomomorphismus*

$$\phi : K[x] \to L \text{ mit } \phi(x) = \alpha,$$

also

$$\phi(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} a_i \alpha^i.$$

Es gibt zwei Fälle:

(1) $\mathrm{Kern}(\phi) = \{0\}$. *Dies ist genau dann der Fall, wenn α transzendent über K ist. In diesem Fall ist $K[\alpha] \simeq K[x]$ und $K(\alpha) \simeq K(x)$.*

(2) $\mathrm{Kern}(\phi) \neq \{0\}$. *Dies ist genau dann der Fall, wenn α algebraisch über K ist. Es gibt ein eindeutig bestimmtes normiertes Polynom $f \in K[x]$ mit*

$$\mathrm{Kern}(\phi) = (f).$$

f heißt das **Minimalpolynom** *von α über K. Das Minimalpolynom ist irreduzibel über K. Man findet dafür auch die Schreibweise $m_{\alpha,K}(x)$. Für $g(x) \in K[x]$ gilt also*

$$g(\alpha) = 0 \quad \Longleftrightarrow \quad g \in (f) \quad \Longleftrightarrow \quad f \mid g.$$

Es gilt

$$K[x]/(f) \simeq K[\alpha] = K(\alpha).$$

Beweis: Das Bild von ϕ ist

$$\mathrm{Bild}(\phi) = \{\sum_{i=0}^{n} a_i \alpha^i : n \in \mathbb{N}_0, a_i \in K\} = K[\alpha].$$

Der Kern von $\phi : K[x] \to L$ ist ein Ideal in $K[x]$. Da $K[x]$ ein Hauptidealring ist, gibt es also ein Polynom f mit

$$\mathrm{Kern}(\phi) = (f).$$

Der Faktorisierungssatz liefert den Isomorphismus

$$K[x]/(f) \simeq K[\alpha].$$

Wir unterscheiden jetzt die Fälle $f = 0$ und $f \neq 0$.

(1) **Fall** $f = 0$**:** Dann ist $K[\alpha] \simeq K[x]$ und $K(\alpha) \simeq K(x)$.

(2) **Fall** $f \neq 0$**:** Wir können annehmen, dass f normiert ist. Damit ist f eindeutig bestimmt.

- Wir zeigen, dass das Polynom f irreduzibel ist. Wegen $\phi(1) = 1 \neq 0$ ist $(f) \neq K[x]$, also $\mathrm{grad}(f) \geq 1$. Wäre f reduzibel, so gäbe es Polynome $g, h \in K[x]$ mit $f = gh$ und $\mathrm{grad}(g) < \mathrm{grad}(f)$ und $\mathrm{grad}(h) < \mathrm{grad}(f)$. Aus $g(\alpha)h(\alpha) = f(\alpha) = 0$ folgt aber $g(\alpha) = 0$ oder $h(\alpha) = 0$, also $g \in \mathrm{Kern}(\phi)$ oder $h \in \mathrm{Kern}(\phi)$, und damit $f \mid g$ oder $f \mid h$, was aber aus Gradgründen nicht sein kann. Daher ist f irreduzibel.
- Für $g \in K[x]$ gilt:

$$g(\alpha) = 0 \quad \Longleftrightarrow \quad g \in \mathrm{Kern}(\phi) \quad \Longleftrightarrow \quad g \in (f) \quad \Longleftrightarrow \quad f \mid g,$$

  wie behauptet.
- Der Faktorisierungssatz liefert $K[x]/(f) \simeq K[\alpha]$. Da f irreduzibel ist, ist (f) ein maximales Ideal in $K[x]$, also $K[x]/(f)$ ein Körper. Also ist auch $K[\alpha]$ ein Körper, was sofort $K[\alpha] = K(\alpha)$ liefert. ■

Bemerkung: Sei $L|K$ eine Körpererweiterung. Aus dem Satz folgt auch sofort folgende Charakterisierung für $\alpha \in L$:

$$\alpha \text{ algebraisch über } K \quad \Longleftrightarrow \quad K[\alpha] = K(\alpha).$$

Das folgende Lemma kann fehlen, Minimalpolynome praktisch zu bestimmen:

LEMMA. *Sei $L|K$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Ist $f \in K[x]$ normiert mit $f(\alpha) = 0$ und ist f irreduzibel über K, so ist f schon das Minimalpolynom von α über K.*

Beweis: Aus $f(\alpha) = 0$ folgt $m_{\alpha,K}(x)|f(x)$ (in $K[x]$), es gibt also ein Polynom $g(x) \in K[x]$ mit

$$f(x) = m_{\alpha,K}(x) \cdot g(x).$$

Da f und $m_{\alpha,K}$ normiert sind, ist auch g normiert. Da f irreduzibel ist, ist $g \in K^*$, also $g = 1$, was die Behauptung beweist. ■

Beispiel: Sei $d \in \mathbb{Q}$ und $\omega \in \mathbb{C}$ mit $\omega^2 = d$, sodass $\omega \notin \mathbb{Q}$ gilt. (Dann ist also $\omega = \pm\sqrt{d}$.) ω ist Nullstelle des Polynoms $x^2 - d \in \mathbb{Q}[x]$. Wäre das Polynom reduzibel über $\mathbb{Q}$, so hätte es eine Nullstelle in $\mathbb{Q}$, d.h. es wäre $\omega \in \mathbb{Q}$, was nicht sein sollte. Also ist $x^2 - d$ irreduzibel über $\mathbb{Q}$, und damit das Minimalpolynom von ω über $\mathbb{Q}$:

$$m_{\omega,\mathbb{Q}}(x) = x^2 - d.$$

4. Wie rechnet man in $K(\alpha)$, wenn man das Minimalpolynom $f \in K[x]$ von α kennt?

SATZ. *Sei $L|K$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K mit Minimalpolynom $f \in K[x]$ vom Grad n.*

(1) *Es gilt*

$$\begin{aligned} K(\alpha) &= \left\{ \sum_{i=0}^{n-1} a_i \alpha^i : a_i \in K \text{ für } i = 0, 1, \ldots, n-1 \right\} = \\ &= \left\{ a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_0, a_1, \ldots, a_{n-1} \in K \right\}. \end{aligned}$$

Jedes Element aus $K(\alpha)$ lässt sich also schreiben als

$$\sum_{i=0}^{n-1} a_i \alpha^i \text{ mit } a_0, \ldots, a_{n-1} \in K.$$

Dabei sind die Koeffizienten $a_0, \ldots, a_{n-1}$ eindeutig bestimmt, d.h.

$$\sum_{i=0}^{n-1} a_i \alpha^i = \sum_{i=0}^{n-1} b_i \alpha^{n-1} \quad \Longleftrightarrow \quad a_i = b_i \text{ für } i = 0, \ldots, n-1.$$

(2) **Addition:**

$$\sum_{i=0}^{n-1} a_i \alpha^i + \sum_{i=0}^{n-1} b_i \alpha^i = \sum_{i=0}^{n-1} (a_i + b_i) \alpha^i.$$

(3) **Multiplikation:** *Dividiert man $(\sum_{i=0}^{n-1} a_i x^i) \cdot (\sum_{i=0}^{n-1} b_i x^i)$ durch $f(x)$, so erhält man eine Darstellung*

$$(\sum_{i=0}^{n-1} a_i x^i) \cdot (\sum_{i=0}^{n-1} x^i) = q(x) f(x) + \sum_{i=0}^{n-1} r_i x^i.$$

Dann gilt:

$$(\sum_{i=0}^{n-1} a_i \alpha^i) \cdot (\sum_{i=0}^{n-1} b_i \alpha^i) = \sum_{i=0}^{n-1} r_i \alpha^i.$$

(4) **Division/Multiplikatives Inverses:** *Ist* $\sum_{i=0}^{n-1} a_i\alpha^i \neq 0$*, so findet man mit dem erweiterten eukldischen Algorithmus* $u, v \in K[x]$ *mit*

$$u(x)f(x) + v(x)(\sum_{i=0}^{n-1} a_i x^i) = 1 \quad \textit{mit} \quad \operatorname{grad}(v) \leq n-1.$$

Schreibt man $v(x) = \sum_{i=0}^{n-1} v_i x^i$*, so gilt*

$$\frac{1}{\sum_{i=0}^{n-1} a_i\alpha^i} = \sum_{i=0}^{n-1} v_i\alpha^i.$$

(5) *Ist* $f = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in K[x]$ *das Minimalpolynom von* α*, so gilt* $f(\alpha) = 0$*, und damit*

$$\alpha^n = -c_0 - c_1\alpha - \cdots - c_{n-1}\alpha^{n-1}.$$

(6) $K(\alpha)$ *ist ein* n*-dimensionaler* K*-Vektorraum mit Basis* $1, \alpha, \ldots, \alpha^{n-1}$.

Beweis: Wir definieren

$$M = \left\{ \sum_{i=0}^{n-1} a_i\alpha^i : a_i \in K \text{ für } i = 0, \ldots, n-1 \right\}.$$

Bevor wir die Gleichheit $K(\alpha) = M$ zeigen, schauen wir uns die Addition, Multiplikation und Division in M an.

(2) Die Formel für die Addition ist klar.

(3) Auch diese Formel ist klar, wobei die zweite Gleichung durch einsetzen von $x = \alpha$ in die Polynomgleichung und $f(\alpha) = 0$ folgt.

(4)
- Da das Minimalpolynom f irreduzibel ist, hat f als normierte Teiler nur 1 und f. Wegen $\sum_{i=0}^{n-1} a_i\alpha^i \neq 0$ ist $\sum_{i=0}^{n-1} a_i x^i$ ein Polynom vom Grad $< n$. Es folgt $\operatorname{ggT}(f, \sum_{i=0}^{n-1} a_i x^i) = 1$. Mit dem erweiterten euklidischen Algorithmus findet man Polynome $u_0, v_0 \in K[x]$ mit

$$u_0(x)f(x) + v_0(x) \cdot (\sum_{i=0}^{n-1} a_i x^i) = 1.$$

- Es ist nicht von vorne herein klar, dass $\operatorname{grad}(v_0) \leq n-1$ gilt. Wir können das aber leicht erreichen. Dividieren wir $v_0(x)$ durch $f(x)$, so erhalten wir eine Darstellung

$$v_0(x) = q(x)f(x) + v(x) \text{ mit } \operatorname{grad}(v) \leq n-1.$$

Es folgt

$$\begin{aligned} 1 &= u_0(x)f(x) + (q(x)f(x) + v(x)) \cdot \sum_{i=0}^{n-1} a_i x^i = \\ &= (u_0(x) + q(x) \cdot \sum_{i=0}^{n-1} a_i x^i)f(x) + v(x) \cdot \sum_{i=0}^{n-1} a_i x^i. \end{aligned}$$

Mit $u(x) = u_0(x) + q(x) \cdot \sum_{i=0}^{n-1} a_i x^i$ folgt

$$u(x)f(x) + v(x) \cdot \sum_{i=0}^{n-1} a_i x^i = 1 \text{ mit } \operatorname{grad}(v) \leq n-1.$$

Diese Gleichung ist im Satz angegeben.

- Schreiben wir jetzt $v(x) = \sum_{i=0}^{n-1} v_i x^i$, so folgt

$$u(x)f(x) + \sum_{i=0}^{n-1} v_i x^i \cdot \sum_{i=0}^{n-1} a_i x^i = 1.$$

Setzen wir jetzt $x = \alpha$ ein, so ergibt sich mit $f(\alpha) = 0$

$$\sum_{i=0}^{n-1} v_i\alpha^i \cdot \sum_{i=0}^{n-1} a_i\alpha^i = 1,$$

und damit die Behauptung.

(1)
- Wir zeigen zunächst mit dem Unterkörper-Kriterium, dass M ein Unterkörper von L ist. Dazu überprüfen wir die einzelnen Punkte, die im Unterkörper-Kriterium stehen:
  (1) $0 \in M$: Klar.
  (2) $x, y \in M \Longrightarrow x + y \in M$: Dies folgt aus der Additionsformeln.
  (3) $x \in M \Longrightarrow -x \in M$: Klar.
  (4) $1 \in M$: Klar.
  (5) $x, y \in M \Longrightarrow xy \in M$: Dies folgt aus der Formeln für die Multiplikation.
  (6) $x \in M \setminus \{0\} \Longrightarrow \frac{1}{x} \in M$: Dies folgt aus den Formeln für die Division.
- Alle Elemente von M liegen in $K(\alpha)$, weswegen trivialerweise $M \subseteq K(\alpha)$ gilt.
- Wir haben gesehen, dass M ein Körper ist, der K und α enthält. Da $K(\alpha)$ der kleinste solche Körper ist, folgt $K(\alpha) \subseteq M$.
- Aus den beiden letzten Punkten ergibt sich die behauptete Gleichheit
$$K(\alpha) = M.$$
- Wir müssen noch zeigen, dass die Darstellung der Elemente von M eindeutig ist. Es gelte
$$\sum_{i=0}^{n-1} a_i \alpha^i = \sum_{i=0}^{n-1} b_i \alpha^i.$$
Dann ist
$$\sum_{i=0}^{n-1} (a_i - b_i) \alpha^i = 0.$$
α ist also Nullstelle des Polynoms
$$g(x) = \sum_{i=0}^{n-1} (a_i - b_i) x^i \in K[x].$$
Da g kleineren Grad als das Minimalpolynom f hat, muss g das Nullpolynom sein, d.h. es gilt $a_i = b_i$ für alle i. Die Umkehrung ist klar.

(5) Aus $f = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ und $f(\alpha) = 0$ folgt
$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1 \alpha + c_0 = 0,$$
und damit
$$\alpha^n = -c_0 - c_1\alpha - \cdots - c_{n-1}\alpha^{n-1}.$$

(6) Wegen $K \subseteq K(\alpha)$ ist klar, dass $K(\alpha)$ ein K-Vektorraum ist. Dass $1, \alpha, \ldots, \alpha^{n-1}$ eine K-Basis ist, folgt aus der in (1) angegebenen Darstellung zusammen mit der Eindeutigkeitsaussage. ■

Bemerkung: Man sieht, dass man in $K(\alpha)$ rechnen kann, wenn man das Minimalpolynom f von α kennt. Aus der Algebra kennt man eine Konstruktion, wie man zu einem Polynom f einen Faktorring $K[x]/(f)$ konstruiert. Der folgende Satz erinnert daran:

SATZ. *Sei K ein Körper und $f \in K[x]$ ein normiertes Polynom vom Grad $n \geq 1$.*

(1) *Es ist*
$$\{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} : a_0, a_1, \ldots, a_{n-1} \in K\}$$
ein Repräsentantensystem für den Faktorring $K[x]/(f)$, insbesondere ist K ein Unterkörper von $K[x]/(f)$.

(2) *Ist α das Bild von x unter der natürlichen Abbildung $K[x] \to K[x]/(f)$, so ist*
$$K[x]/(f) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_0, a_1, \ldots, a_{n-1} \in K\}.$$
$K[x]/(f)$ ist ein n-dimensionaler K-Vektorraum mit Basis $1, \alpha, \ldots, \alpha^{n-1}$. Ist $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, so genügt α der Gleichung
$$\alpha^n = -c_0 - c_1\alpha - \cdots - c_{n-1}\alpha^{n-1}.$$

(3) *Ist f irreduzibel, so ist $K[x]/(f)$ ein Körper und f ist das Minimalpolynom von α über K.*

5. Die Charakteristik eines Körpers

Sei K ein Körper. Es gibt genau einen Ringhomomorphismus

$$\phi : \mathbb{Z} \to K,$$

der durch $\phi(1) = 1_K$ festgelegt ist. Der Kern ist ein Ideal in $\mathbb{Z}$.

- **Fall** $\mathrm{Kern}(\phi) = \{0\}$**:** Wir sagen, K **hat Charakteristik** 0 und schreiben $\mathrm{char}(K) = 0$. Für alle $n \in \mathbb{N}$ ist

  $$n \cdot 1_K = \sum_{i=1}^{n} 1_K \neq 0.$$

  Es ist $\phi(\mathbb{Z}) \simeq \mathbb{Z}$. Wir können $\mathbb{Z}$ als Unterring von R auffassen. Durch

  $$\widetilde{\phi} : \mathbb{Q} \to K, \quad \frac{a}{b} \mapsto \frac{a \cdot 1_K}{b \cdot 1_K}$$

  wird ein Homomorphismus definiert. Wir können daher $\mathbb{Q}$ als Unterkörper von K auffassen. Es ist dann der kleinste Unterkörper von K, man nennt ihn auch den **Primkörper** von K.
- **Fall** $\mathrm{Kern}(\phi) = \mathbb{Z}n$ **mit** $n \in \mathbb{N}$**:** Wegen $\phi(1) = 1 \neq 0$ ist $n \geq 2$. Wäre n keine Primzahl, so könnte man zerlegen $n = n_1 n_2$ mit $n_1, n_2 \in \mathbb{N}_{\geq 2}$ und würde erhalten

  $$0 = \phi(n) = \phi(n_1 n_2) = \phi(n_1)\phi(n_2),$$

  also $\phi(n_1) = 0$ oder $\phi(n_2) = 0$, und damit $n_1 \in \mathrm{Kern}(\phi)$ oder $n_2 \in \mathrm{Kern}(\phi)$, also $n \mid n_1$ oder $n \mid n_2$, was natürlich nicht der Fall ist. Also ist $n = p$ eine Primzahl. Dann ist $\phi(\mathbb{Z}) \simeq \mathbb{Z}/(p) \simeq \mathbb{Z}_p = \mathbb{F}_p$. Wir können also $\mathbb{Z}_p$ als Unterring von K auffassen. Insbesondere ist dann $\mathbb{F}_p = \mathbb{Z}_p$ der kleinste Unterkörper von K, also der **Primkörper** von K. Wir sagen K hat **Charakteristik** p, wir schreiben auch $\mathrm{char}(K) = p$.

Lemma (Frobenius-Homomorphismus). *Ist K ein Körper der Charakteristik p (mit einer Primzahl p), so ist*

$$\phi : K \to K \text{ mit } \phi(a) = a^p$$

ein Ringhomomorphismus, insbesondere gilt für $a, b \in K$

$$(a+b)^p = a^p + b^p, \quad (ab)^p = a^p b^p.$$

Beweis: Für $i \in \mathbb{N}$ mit $1 \leq i \leq p-1$ gilt für den Binomialkoeffizienten

$$\binom{p}{i} = \frac{p \cdot (p-1) \ldots (p-(i-1))}{1 \cdot 2 \ldots i}.$$

Da im Nenner p nicht vorkommt, ist $\binom{p}{i}$ durch p teilbar, also ein Vielfaches von p. Da in K die Gleichung $p = 0$ gilt, folgt

$$\binom{p}{i} = 0 \text{ in } K \text{ für } 1 \leq i \leq p-1.$$

Mit dem binomischen Lehrsatz erhalten wir für $a, b \in K$

$$(a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i + b^p = a^p + b^p.$$

Die restlichen Aussagen sind klar. ■

6. Erinnerung: Faktorringe

Der **Faktorring** $R/\mathfrak{a}$**:** Sei R ein kommutativer Ring und $\mathfrak{a}$ ein Ideal in R.

(1) Durch
$$x \equiv y \bmod \mathfrak{a} \quad \Longleftrightarrow \quad x - y \in \mathfrak{a}$$
wird eine Äquivalenzrelation auf R definiert, die **Kongruenz modulo** $\mathfrak{a}$. Die Äquivalenzklasse von x bezeichnen wir mit $\overline{x}$. Als Menge ist
$$\overline{x} = x + \mathfrak{a} = \{x + a : a \in \mathfrak{a}\}.$$
Es gilt dann
$$x \equiv y \bmod \mathfrak{a} \quad \Longleftrightarrow \quad \overline{x} = \overline{y}.$$
Sei $R/\mathfrak{a}$ die Menge der Äquivalenzklassen, also
$$R/\mathfrak{a} = \{\overline{x} : x \in R\}.$$
Die kanonische Abbildung
$$\pi : R \to R/\mathfrak{a} \text{ mit } \pi(x) = \overline{x}$$
ist offensichtlich surjektiv.

(2) **Addition:** Seien $x, x', y, y' \in R$ mit
$$x \equiv x' \bmod \mathfrak{a} \quad \text{und} \quad y \equiv y' \bmod \mathfrak{a}.$$
Dann gibt es $a, b \in \mathfrak{a}$ mit
$$x' = x + a, \quad y' = y + b.$$
Es folgt $(x' + y') - (x + y) = a + b \in \mathfrak{a}$, also
$$x + y \equiv x' + y' \bmod \mathfrak{a}.$$
Anders geschrieben:
$$\overline{x} = \overline{x'} \text{ und } \overline{y} = \overline{y'} \quad \Longrightarrow \quad \overline{x + y} = \overline{x' + y'}.$$
Daher wird durch
$$\overline{x} + \overline{y} = \overline{x + y}$$
eine wohldefinierte Verknüpfung (Addition) auf $R/\mathfrak{a}$ definiert. Man überprüft, dass $(R/\mathfrak{a}, +)$ eine abelsche Gruppe mit neutralem Element $\overline{0}$ ist. (Für das additive Inverse gilt $-\overline{x} = \overline{-x}$.)

(3) **Multiplikation:** Seien $x, x', y, y' \in R$ mit
$$x \equiv x' \bmod \mathfrak{a} \quad \text{und} \quad y \equiv y' \bmod \mathfrak{a}.$$
Dann gibt es $a, b \in \mathfrak{a}$ mit
$$x' = x + a, \quad y' = y + b.$$
Es folgt
$$x'y' - xy = (x + a)(y + b) - xy = (xy + xb + ay + ab) - (xy) = xb + ay + ab \in \mathfrak{a}$$
wegen $xb, ay, ab \in \mathfrak{a}$, also
$$xy \equiv x'y' \bmod \mathfrak{a}.$$
Anders geschrieben:
$$\overline{x} = \overline{x'} \text{ und } \overline{y} = \overline{y'} \quad \Longrightarrow \quad \overline{xy} = \overline{x'y'}.$$
Daher wird durch
$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$
eine wohldefinierte Verknüpfung (Multiplikation) auf $R/\mathfrak{a}$ definiert. Wir zeigen, dass $(R/\mathfrak{a}, \cdot)$ ein Monoid ist:

- Es gilt das Assoziativgesetz:
$$\overline{x} \cdot (\overline{y} \cdot \overline{z}) = \overline{x} \cdot \overline{y \cdot z} = \overline{x \cdot (y \cdot z)} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot y} \cdot \overline{z} = (\overline{x} \cdot \overline{y}) \cdot \overline{z}.$$
- $\overline{1}$ ist neutrales Element der Multiplikation:
$$\overline{1} \cdot \overline{x} = \overline{1 \cdot x} = \overline{x} = \overline{x \cdot 1} = \overline{x} \cdot \overline{1}.$$

(4) Es gelten die Distributivgesetze:

$$\overline{x} \cdot (\overline{y} + \overline{z}) = \overline{x} \cdot \overline{y+z} = \overline{x \cdot (y+z)} = \overline{x \cdot y + x \cdot z} = \overline{x \cdot y} + \overline{x \cdot z} = \overline{x} \cdot \overline{y} + \overline{x} \cdot \overline{z},$$
$$(\overline{x} + \overline{y}) \cdot \overline{z} = \overline{x+y} \cdot \overline{z} = \overline{(x+y) \cdot z} = \overline{x \cdot z + y \cdot z} = \overline{x \cdot z} + \overline{y \cdot z} = \overline{x} \cdot \overline{z} + \overline{y} \cdot \overline{z}.$$

(5) Daher ist $(R/\mathfrak{a}, +, \cdot)$ ein kommutativer Ring, der **Faktorring** von R nach $\mathfrak{a}$ oder von R modulo $\mathfrak{a}$. Die Abbildung $\pi : R \to R/\mathfrak{a}$ mit $\pi(x) = \overline{x}$ wird auch als kanonische Abbildung bezeichnet und ist ein surjektiver Ringhomomorphismus mit Kern $\mathfrak{a}$.

Bemerkungen: Im Fall $\mathfrak{a} = \{0\}$ gilt:

$$\overline{x} = \overline{y} \quad \Longleftrightarrow \quad x \equiv y \bmod \mathfrak{a} \quad \Longleftrightarrow \quad x - y \in \{0\} \quad \Longleftrightarrow \quad x = y,$$

Wir können also $R/\{0\}$ mit R identifizieren.
Im Fall $\mathfrak{a} = R$ gilt für $x \in R$:

$$x \in R \quad \Longrightarrow \quad x \in \mathfrak{a} \quad \Longrightarrow \quad x \equiv 0 \bmod \mathfrak{a} \quad \Longrightarrow \quad \overline{x} = \overline{0}.$$

R/R besteht also nur aus einem Element, ist daher der Nullring.

Beispiel: Wir betrachten in $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ das Ideal $\mathfrak{a} = (1+i)$. Wegen $(1-i)(1+i) = 2$ ist $2 \in \mathfrak{a}$. Daher haben wir

$$2 \equiv 0 \bmod \mathfrak{a} \quad \text{und} \quad i \equiv -1 \equiv 1 \bmod \mathfrak{a}.$$

Es ist also

$$a + bi \equiv a + b \equiv ((a+b) \bmod 2) \bmod \mathfrak{a}.$$

Es gibt also höchstens die Restklassen $\overline{0}$ und $\overline{1}$ modulo $\mathfrak{a}$. Es gilt

$$\begin{aligned}
\overline{1} = \overline{0} \quad &\Longleftrightarrow \quad 1 \equiv 0 \bmod \mathfrak{a} \quad \Longleftrightarrow \quad 1 \in \mathfrak{a} \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad 1 = (a+bi)(1+i) \text{ mit Zahlen } a, b \in \mathbb{Z} \quad \Longrightarrow \\
&\Longrightarrow \quad 1 = |a+bi|^2 \cdot |1+i|^2 \text{ mit Zahlen } a, b \in \mathbb{Z} \quad \Longrightarrow \\
&\Longrightarrow \quad 1 = (a^2+b^2) \cdot 2 \text{ mit Zahlen } a, b \in \mathbb{Z}.
\end{aligned}$$

Die rechte Seite ist aber falsch, da 1 kein Vielfaches von 2 in $\mathbb{Z}$ ist. Also gilt

$$\overline{1} \neq \overline{0}, \quad \text{und damit} \quad \mathbb{Z}[i]/(1+i) = \{\overline{0}, \overline{1}\}.$$

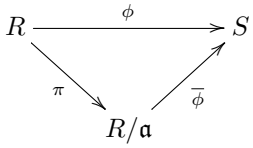
Satz (Faktorisierungssatz). *Sei $\phi : R \to S$ ein Ringhomomorphismus und $\mathfrak{a} \subseteq R$ ein Ideal mit $\mathfrak{a} \subseteq \mathrm{Kern}(\phi)$. Dann gibt es genau einen Ringhomomorphismus*

$$\overline{\phi} : R/\mathfrak{a} \to S,$$

sodass gilt

$$\phi = \overline{\phi} \circ \pi.$$

ϕ „faktorisiert“ also über $R/\mathfrak{a}$. Dies drückt sich auch in folgendem sogenannten kommutativen Diagramm aus:



Weiter gilt:

- *Ist $\mathfrak{a} = \mathrm{Kern}(\phi)$, so ist $\overline{\phi} : R/\mathrm{Kern}(\phi) \to S$ injektiv.*
- *Ist $\mathfrak{a} = \mathrm{Kern}(\phi)$ und ϕ surjektiv, so ist $\overline{\phi}$ ein Isomorphismus:*

$$R/\mathrm{Kern}(\phi) \xrightarrow{\simeq} S.$$

Beweis:

- *Eindeutigkeit:* Ist $\overline{\phi}$ mit $\phi = \overline{\phi} \circ \pi$, so gilt für $x \in R$
$$\phi(x) = (\overline{\phi} \circ \pi)(x) = \overline{\phi}(\pi(x)) = \overline{\phi}(\overline{x}).$$
$\overline{\phi}$ ist also durch ϕ eindeutig bestimmt.
- *Existenz:* Seien $x, x' \in R$ mit $\overline{x} = \overline{x'}$. Dann gilt $x \equiv x' \bmod \mathfrak{a}$, d.h. es gibt ein $a \in \mathfrak{a}$ mit $x' = x + a$. Nach Voraussetzung ist $\mathfrak{a} \subseteq \mathrm{Kern}(\phi)$, also $\phi(a)0$, und damit $\phi(x') = \phi(x)$. Daher ist $\overline{\phi} : R/\mathfrak{a} \to R$ durch
$$\overline{\phi}(\overline{x}) = \phi(x)$$
wohldefiniert. Dass $\overline{\phi}$ ein Ringhomomorphismus ist, rechnet man nun einfach nach.
- *Fall* $\mathrm{Kern}(\phi) = \mathfrak{a}$*:* Sei $\overline{\phi}(\overline{x}) = \overline{\phi}(\overline{y})$. Dann ist $\phi(x) = \phi(y)$, also $\phi(y - x) = 0$ und damit $y - x \in \mathrm{Kern}(\phi) = \mathfrak{a}$, also $x \equiv y \bmod \mathfrak{a}$ und damit $\overline{x} = \overline{y}$. Dies beweist die Injektivität von $\overline{\phi}$.
- Der Rest ist dann klar. ■

Beispiel: Ist $n \in \mathbb{N}$, so wird durch
$$\mathbb{Z} \to \mathbb{Z}_n, \quad a \mapsto (a \bmod n)$$
ein surjektiver Ringhomomorphismus definiert mit Kern $\mathbb{Z}\, n = (n)$. Daher gilt
$$\mathbb{Z}/(n) \simeq \mathbb{Z}_n.$$
Statt $\mathbb{Z}_n$ findet man auch oft die Schreibweise $\mathbb{Z}/(n)$ oder $\mathbb{Z}/n\mathbb{Z}$ oder $\mathbb{Z}/\mathbb{Z}n$.

Der folgende Satz zeigt eine Möglichkeit, aus bekannten Ringen neue Ringe zu gewinnen.

Satz. *Sei R ein kommutativer Ring und $f \in R[x]$ ein normiertes Polynom vom Grad $n \geq 1$.*

(1) *Dann ist*
$$\{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} : a_0, a_1, \ldots, a_{n-1} \in R\}$$
ein Repräsentantensystem für den Faktorring $R[x]/(f)$, insbesondere kann man R als Unterring von $R[x]/(f)$ auffassen.

(2) *Ist ξ das Bild von x in $R[x]/(f)$, so ist*
$$R[x]/(f) = \{a_0 + a_1 \xi + \cdots + a_{n-1} \xi^{n-1} : a_0, a_1, \ldots, a_{n-1} \in R\}.$$
Ist $f(x) = x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$, so genügt ξ der Gleichung
$$\xi^n = -c_0 - c_1 \xi - \cdots - c_{n-1} \xi^{n-1}.$$

(3) *Ist $R = K$ ein Körper, so ist $1, \xi, \ldots, \xi^{n-1}$ eine K-Basis von $K[x]/(f)$.*

Beweis:

(1) Sei $a(x) \in R[x]$ ein beliebiges Polynom. Dividieren wir durch $f = x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$, so erhalten wir eine Darstellung
$$a(x) = b(x) f(x) + (a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) \text{ mit } b(x) \in R[x] \text{ und } a_0, a_1, \ldots, a_{n-1} \in R.$$
Dann ist
$$a(x) \equiv a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \bmod (f).$$
Gilt nun
$$a_0 + a_1 x + \cdots + a_n x^{n-1} \equiv b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} \bmod (f),$$
so gibt es ein Polynom $g(x) \in R[x]$ mit
$$(a_0 - b_0) + (a_1 - b_1) x + \cdots + (a_{n-1} - b_{n-1}) x^{n-1} = g(x) f(x).$$
Wäre $g(x) \neq 0$, so wäre $\mathrm{grad}(g(x) f(x)) = \mathrm{grad}(g(x)) + \mathrm{grad}(f(x)) \geq \mathrm{grad}(f(x)) = n$, was offensichtlich nicht sein kann. Also ist $g(x) = 0$ und damit
$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}.$$
Daher ist
$$\{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} : a_0, a_1, \ldots, a_{n-1} \in R\}$$

ein Repräsentantensystem von $R[x]/(f)$. Insbesondere gilt für $a, a' \in R$

$$\overline{a} = \overline{a'} \quad \Longleftrightarrow \quad a = a'.$$

Wir können also R auch als Teilmenge von $R[x]/(f)$ auffassen und schreiben $\overline{a} = a$ für $a \in R$.

(2) Mit $\xi = \overline{x}$ gilt dann

$$\begin{aligned} R[x]/(f) &= \{\overline{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}} : a_0, a_1, \ldots, a_{n-1} \in R\} = \\ &= \{a_0 + a_1\overline{x} + \cdots + a_{n-1}\overline{x}^{n-1} : a_0, a_1, \ldots, a_{n-1} \in R\} = \\ &= \{a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1} : a_0, a_1, \ldots, a_{n-1} \in R\}. \end{aligned}$$

Nun gilt

$$c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + x^n \equiv 0 \bmod (f),$$

also

$$\begin{aligned} 0 &= \overline{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + x^n} = c_0 + c_1\overline{x} + \cdots + c_{n-1}\overline{x}^{n-1} + \overline{x}^n = \\ &= c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1} + \xi^n, \end{aligned}$$

woraus

$$\xi^n = -c_0 - c_1\xi - \cdots - c_{n-1}\xi^{n-1}$$

folgt.

(3) Dies folgt aus (1). ■

Bemerkung: Wir multipliziert man in $R[x]/(f)$? Hat man $g, h \in R[x]$ vom Grad $< n$ und will einen Repräsentanten für $g(\xi)h(\xi)$ finden, so kann man die Relation $\xi^n = -c_0 - c_1\xi - \cdots - c_{n-1}\xi^{n-1}$ benutzen, bis man nur noch eine Linearkombination von $1, \xi, \ldots, \xi^{n-1}$ hat. Man kann aber auch $g(x)h(x)$ durch $f(x)$ dividieren:

$$g(x)h(x) = q(x)f(x) + r(x) \text{ mit } \operatorname{grad}(r) < n.$$

Dann ist $g(\xi)h(\xi) = r(\xi)$.

7. Anhang: Irreduzibilitätskriterien für Polynome aus $\mathbb{Q}[x]$

Satz (Eisenstein-Kriterium). *Sei $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ ein Polynom vom Grad $n \geq 1$. Ist p eine Primzahl mit*

$$p \nmid a_n, \quad p \mid a_{n-1}, \quad p \mid a_{n-2}, \quad \ldots \quad p \mid a_1, \quad p \mid a_0 \quad \text{und} \quad p^2 \nmid a_0,$$

so ist f irreduzibel in $\mathbb{Q}[x]$.

Beispiele:

(1) Ist $a \in \mathbb{Z}$ und gibt es eine Primzahl p mit $p \mid a$, aber $p^2 \nmid a$, so ist für alle $n \in \mathbb{N}$ das Polynom

$$x^n - a$$

irreduzibel über $\mathbb{Q}$.

(2) Das Polynom $3x^5 - 15$ ist irreduzibel über $\mathbb{Q}$, nicht jedoch über $\mathbb{Z}$.

Satz (Reduktionskriterium). *Sei $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ vom Grad $n \geq 1$, p eine Primzahl mit $p \nmid a_n$. Sei*

$$\overline{f} = \overline{a_n}x^n + \cdots + \overline{a_1}x + \overline{a_0} \in \mathbb{F}_p[x].$$

Ist das modulo p reduzierte Polynom $\overline{f}$ irreduzibel, so ist f über $\mathbb{Q}$ irreduzibel.

Beispiel: Das Polynom $x^2 + x + 1$ ist irreduzibel über $\mathbb{F}_2$, da es keine Nullstelle in $\mathbb{F}_2$ hat. Daher ist auch jedes Polynom

$$f = ax^2 + bx + c \in \mathbb{Z}[x] \quad \text{mit } a \equiv b \equiv c \equiv 1 \bmod 2$$

über $\mathbb{Q}$ irreduzibel, wie man durch Reduktion modulo 2 sieht.

SATZ (Integral Root Test). *Sei $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ ein normiertes Polynom vom Grad $n \geq 1$. Ist $\alpha \in \mathbb{Q}$ eine Nullstelle von f, d.h. $f(\alpha) = 0$, so gilt:*

$$\alpha \in \mathbb{Z} \quad \textit{und} \quad \alpha \mid a_0.$$

Beispiel: Wir betrachten das Polynom

$$f = x^3 + x + 2 \in \mathbb{Z}[x].$$

Der vorangegangene Satz sagt, dass Nullstellen aus $\mathbb{Q}$ schon in $\mathbb{Z}$ liegen und Teiler von 2 sind. Also kommen nur $\pm 1, \pm 2$ als rationale Nullstellen in Frage. Nun ist

$$f(1) = 4, \quad f(-1) = 0, \quad f(2) = 12, \quad f(-2) = -8.$$

Also ist -1 eine Nullstelle von f und daher spaltet $x + 1$ ab:

$$f = (x + 1)(x^2 - x + 2).$$

Mit der gleichen Vorgehensweise findet man, dass $x^2 - x + 2$ keine Nullstelle in $\mathbb{Q}$ hat, weswegen das Polynom irreduzibel über $\mathbb{Q}$ ist. Daher ist

$$f = (x + 1)(x^2 - x + 2)$$

die Primfaktorzerlegung von f über $\mathbb{Q}$ (und $\mathbb{Z}$).

8. Anhang: Die Zerlegungen der normierten Polynome vom Grad ≤ 4 aus $\mathbb{F}_2[x]$ und $\mathbb{F}_3[x]$

Hier sind die Zerlegungen der normierten Polynome aus $\mathbb{F}_2[x]$ vom Grad ≤ 4:

$f \in \mathbb{F}_2[x]$	Zerlegung
x^2	x^2
$x^2 + 1$	$(x+1)^2$
$x^2 + x$	$x \cdot (x+1)$
$x^2 + x + 1$	irreduzibel
x^3	x^3
$x^3 + 1$	$(x+1) \cdot (x^2 + x + 1)$
$x^3 + x$	$x \cdot (x+1)^2$
$x^3 + x + 1$	irreduzibel
$x^3 + x^2$	$(x+1) \cdot x^2$
$x^3 + x^2 + 1$	irreduzibel
$x^3 + x^2 + x$	$x \cdot (x^2 + x + 1)$
$x^3 + x^2 + x + 1$	$(x+1)^3$

$f \in \mathbb{F}_2[x]$	Zerlegung
x^4	x^4
$x^4 + 1$	$(x+1)^4$
$x^4 + x$	$x \cdot (x+1) \cdot (x^2 + x + 1)$
$x^4 + x + 1$	irreduzibel
$x^4 + x^2$	$x^2 \cdot (x+1)^2$
$x^4 + x^2 + 1$	$(x^2 + x + 1)^2$
$x^4 + x^2 + x$	$x \cdot (x^3 + x + 1)$
$x^4 + x^2 + x + 1$	$(x+1) \cdot (x^3 + x^2 + 1)$
$x^4 + x^3$	$(x+1) \cdot x^3$
$x^4 + x^3 + 1$	irreduzibel
$x^4 + x^3 + x$	$x \cdot (x^3 + x^2 + 1)$
$x^4 + x^3 + x + 1$	$(x+1)^2 \cdot (x^2 + x + 1)$
$x^4 + x^3 + x^2$	$x^2 \cdot (x^2 + x + 1)$
$x^4 + x^3 + x^2 + 1$	$(x+1) \cdot (x^3 + x + 1)$
$x^4 + x^3 + x^2 + x$	$x \cdot (x+1)^3$
$x^4 + x^3 + x^2 + x + 1$	irreduzibel

Hier sind die Zerlegungen der normierten Polynome aus $\mathbb{F}_3[x]$ vom Grad ≤ 4:

$f \in \mathbb{F}_3[x]$	Zerlegung
x^2	x^2
x^2+1	irreduzibel
x^2+2	$(x+1)\cdot(x+2)$
x^2+x	$x\cdot(x+1)$
x^2+x+1	$(x+2)^2$
x^2+x+2	irreduzibel
x^2+2x	$x\cdot(x+2)$
x^2+2x+1	$(x+1)^2$
x^2+2x+2	irreduzibel
x^3	x^3
x^3+1	$(x+1)^3$
x^3+2	$(x+2)^3$
x^3+x	$x\cdot(x^2+1)$
x^3+x+1	$(x+2)\cdot(x^2+x+2)$
x^3+x+2	$(x+1)\cdot(x^2+2x+2)$
x^3+2x	$x\cdot(x+1)\cdot(x+2)$
x^3+2x+1	irreduzibel
x^3+2x+2	irreduzibel
x^3+x^2	$(x+1)\cdot x^2$
x^3+x^2+1	$(x+2)\cdot(x^2+2x+2)$
x^3+x^2+2	irreduzibel
x^3+x^2+x	$x\cdot(x+2)^2$
x^3+x^2+x+1	$(x+1)\cdot(x^2+1)$
x^3+x^2+x+2	irreduzibel
x^3+x^2+2x	$x\cdot(x^2+x+2)$
x^3+x^2+2x+1	irreduzibel
x^3+x^2+2x+2	$(x+2)\cdot(x+1)^2$
x^3+2x^2	$(x+2)\cdot x^2$
x^3+2x^2+1	irreduzibel
x^3+2x^2+2	$(x+1)\cdot(x^2+x+2)$
x^3+2x^2+x	$x\cdot(x+1)^2$
x^3+2x^2+x+1	irreduzibel
x^3+2x^2+x+2	$(x+2)\cdot(x^2+1)$
x^3+2x^2+2x	$x\cdot(x^2+2x+2)$
x^3+2x^2+2x+1	$(x+1)\cdot(x+2)^2$
x^3+2x^2+2x+2	irreduzibel
x^4	x^4
x^4+1	$(x^2+x+2)\cdot(x^2+2x+2)$
x^4+2	$(x+1)\cdot(x+2)\cdot(x^2+1)$
x^4+x	$x\cdot(x+1)^3$
x^4+x+1	$(x+2)\cdot(x^3+x^2+x+2)$
x^4+x+2	irreduzibel
x^4+2x	$x\cdot(x+2)^3$
x^4+2x+1	$(x+1)\cdot(x^3+2x^2+x+1)$
x^4+2x+2	irreduzibel
x^4+x^2	$x^2\cdot(x^2+1)$
x^4+x^2+1	$(x+1)^2\cdot(x+2)^2$
x^4+x^2+2	irreduzibel
x^4+x^2+x	$x\cdot(x+2)\cdot(x^2+x+2)$
x^4+x^2+x+1	irreduzibel
x^4+x^2+x+2	$(x+1)\cdot(x^3+2x^2+2x+2)$
x^4+x^2+2x	$x\cdot(x+1)\cdot(x^2+2x+2)$
x^4+x^2+2x+1	irreduzibel
x^4+x^2+2x+2	$(x+2)\cdot(x^3+x^2+2x+1)$
x^4+2x^2	$(x+1)\cdot(x+2)\cdot x^2$
x^4+2x^2+1	$(x^2+1)^2$
x^4+2x^2+2	irreduzibel
x^4+2x^2+x	$x\cdot(x^3+2x+1)$
x^4+2x^2+x+1	$(x+1)\cdot(x^3+2x^2+1)$

$f \in \mathbb{F}_3[x]$	Zerlegung
x^4+2x^2+x+2	$(x+2)^2\cdot(x^2+2x+2)$
x^4+2x^2+2x	$x\cdot(x^3+2x+2)$
x^4+2x^2+2x+1	$(x+2)\cdot(x^3+x^2+2)$
x^4+2x^2+2x+2	$(x+1)^2\cdot(x^2+x+2)$
x^4+x^3	$(x+1)\cdot x^3$
x^4+x^3+1	$(x+2)\cdot(x^3+2x^2+2x+2)$
x^4+x^3+2	irreduzibel
x^4+x^3+x	$x\cdot(x+2)\cdot(x^2+2x+2)$
x^4+x^3+x+1	$(x+1)^4$
x^4+x^3+x+2	$(x^2+1)\cdot(x^2+x+2)$
x^4+x^3+2x	$x\cdot(x^3+x^2+2)$
x^4+x^3+2x+1	irreduzibel
x^4+x^3+2x+2	$(x+1)\cdot(x+2)^3$
$x^4+x^3+x^2$	$x^2\cdot(x+2)^2$
$x^4+x^3+x^2+1$	irreduzibel
$x^4+x^3+x^2+2$	$(x+1)^2\cdot(x^2+2x+2)$
$x^4+x^3+x^2+x$	$x\cdot(x+1)\cdot(x^2+1)$
$x^4+x^3+x^2+x+1$	irreduzibel
$x^4+x^3+x^2+x+2$	$(x+2)\cdot(x^3+2x^2+1)$
$x^4+x^3+x^2+2x$	$x\cdot(x^3+x^2+x+2)$
$x^4+x^3+x^2+2x+1$	$(x+1)\cdot(x+2)\cdot(x^2+x+2)$
$x^4+x^3+x^2+2x+2$	irreduzibel
$x^4+x^3+2x^2$	$x^2\cdot(x^2+x+2)$
$x^4+x^3+2x^2+1$	$(x+1)\cdot(x^3+2x+1)$
$x^4+x^3+2x^2+2$	$(x+2)\cdot(x^3+2x^2+x+1)$
$x^4+x^3+2x^2+x$	$x\cdot(x^3+x^2+2x+1)$
$x^4+x^3+2x^2+x+1$	$(x+2)^2\cdot(x^2+1)$
$x^4+x^3+2x^2+x+2$	$(x+1)\cdot(x^3+2x+2)$
$x^4+x^3+2x^2+2x$	$x\cdot(x+2)\cdot(x+1)^2$
$x^4+x^3+2x^2+2x+1$	$(x^2+2x+2)^2$
$x^4+x^3+2x^2+2x+2$	irreduzibel
x^4+2x^3	$(x+2)\cdot x^3$
x^4+2x^3+1	$(x+1)\cdot(x^3+x^2+2x+1)$
x^4+2x^3+2	irreduzibel
x^4+2x^3+x	$x\cdot(x^3+2x^2+1)$
x^4+2x^3+x+1	irreduzibel
x^4+2x^3+x+2	$(x+2)\cdot(x+1)^3$
x^4+2x^3+2x	$x\cdot(x+1)\cdot(x^2+x+2)$
x^4+2x^3+2x+1	$(x+2)^4$
x^4+2x^3+2x+2	$(x^2+1)\cdot(x^2+2x+2)$
$x^4+2x^3+x^2$	$x^2\cdot(x+1)^2$
$x^4+2x^3+x^2+1$	irreduzibel
$x^4+2x^3+x^2+2$	$(x+2)^2\cdot(x^2+x+2)$
$x^4+2x^3+x^2+x$	$x\cdot(x^3+2x^2+x+1)$
$x^4+2x^3+x^2+x+1$	$(x+1)\cdot(x+2)\cdot(x^2+2x+2)$
$x^4+2x^3+x^2+x+2$	irreduzibel
$x^4+2x^3+x^2+2x$	$x\cdot(x+2)\cdot(x^2+1)$
$x^4+2x^3+x^2+2x+1$	irreduzibel
$x^4+2x^3+x^2+2x+2$	$(x+1)\cdot(x^3+x^2+2)$
$x^4+2x^3+2x^2$	$x^2\cdot(x^2+2x+2)$
$x^4+2x^3+2x^2+1$	$(x+2)\cdot(x^3+2x+2)$
$x^4+2x^3+2x^2+2$	$(x+1)\cdot(x^3+x^2+x+2)$
$x^4+2x^3+2x^2+x$	$x\cdot(x+1)\cdot(x+2)^2$
$x^4+2x^3+2x^2+x+1$	$(x^2+x+2)^2$
$x^4+2x^3+2x^2+x+2$	irreduzibel
$x^4+2x^3+2x^2+2x$	$x\cdot(x^3+2x^2+2x+2)$
$x^4+2x^3+2x^2+2x+1$	$(x+1)^2\cdot(x^2+1)$
$x^4+2x^3+2x^2+2x+2$	$(x+2)\cdot(x^3+2x+1)$