Inhaltsverzeichnis

Blatt 2, Aufgabe 4

Sei G eine Gruppe.

Behauptung. *Folgende Aussagen sind äquivalent:*

(α) *G ist abelsch.*

(β) *$(ab)^2 = a^2b^2$ für alle $a, b \in G$.*

(γ) *$(ab)^{-1} = a^{-1}b^{-1}$ für alle $a, b \in G$.*

Beweis. „(α) $\Rightarrow$ (β)“: Seien $a, b \in G$ beliebig. Dann gilt

$$(ab)^2 = (ab)(ab) = abab \overset{(\star)}{=} aabb = a^2b^2,$$

wobei in Schritt ($\star$) die Voraussetzung der Kommutativität von G eingeht.

„(β) $\Rightarrow$ (α)“: Seien $a, b \in G$ beliebig. Dann gilt

$$(ab)^2 = a^2b^2 \quad \Rightarrow \quad abab = aabb \quad \overset{(\diamond)}{\Rightarrow} \quad ba = ab,$$

wobei wir in Schritt ($\diamond$) zuerst das a von links und dann das b von rechts gekürzt haben. (Dass man das machen kann, sagt die sog. Kürzungsregel. Man kann den Schritt auch noch anders begründen, nämlich durch Multiplikation mit a^{-1} von links und b^{-1} von rechts.)

„(α) $\Rightarrow$ (γ)“: Seien $a, b \in G$ beliebig. Dann gilt

$$(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1},$$

wobei der erste Schritt eine allgemeingültige Rechenregel in Gruppen ist (wurde in der Vorlesung bewiesen) und im zweiten Schritt die Voraussetzung eingeht.

„(γ) $\Rightarrow$ (α)“: Seien $a, b \in G$ beliebig. Dann folgt aus der Gleichung $(ab)^{-1} = a^{-1}b^{-1}$ durch Invertieren von linker und rechter Seite die Rechnung

$$ab = ((ab)^{-1})^{-1} = (a^{-1}b^{-1})^{-1} = (b^{-1})^{-1}\,(a^{-1})^{-1} = ba. \qquad \square$$

Warnung zu Blatt 3, Aufgabe 3

In der Globalübung wurden folgende zwei Aussagen gezeigt:

1. Sind x und g beliebige Elemente einer beliebigen Gruppe, so ist $g^{-1}xg$ von derselben Ordnung wie x.
2. Speziell in Permutationsgruppen $S(n)$ sind Zyklen der Länge k Elemente von Ordnung k.

Daraus folgt aber noch nicht folgende Behauptung:

Behauptung. *Ist $\xi \in S(n)$ ein Zyklus der Länge k und $\pi \in S(n)$ beliebig, so ist auch $\pi^{-1}\xi\pi \in S(n)$ ein Zyklus der Länge k.*

Nach 2. gilt zwar, dass ein solches ξ ein Element der Ordnung k ist, womit nach 1. auch $\pi^{-1}\xi\pi$ ein Element der Ordnung k ist; daraus folgt aber noch nicht, dass $\pi^{-1}\xi\pi$ wirklich ein Zyklus der Länge k ist!

Das liegt daran, dass die Umkehrung in 2. nicht gilt. Es gibt also in $S(n)$ Permutationen der Ordnung k, die nicht Zyklen der Länge k sind: Zum Beispiel hat

$$\sigma := (1\ 2)\,(3\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S(4)$$

Ordnung 2, da

$$\sigma^1 \neq e \quad \text{und} \quad \sigma^2 = e,$$

aber σ selbst in kein Zyklus der Länge 2.

Blatt 3, Aufgabe 4

Sei die Teilmenge

$$\mathcal{C} := \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \middle| \, x, y \in \mathbb{R} \right\}$$

der reellen (2×2)-Matrizen definiert.

Behauptung (a)**.** *Bezüglich der Matrizenaddition ist $\mathcal{C}$ eine abelsche Gruppe.*

Beweis. Dazu müssen wir die Gruppenaxiome nachrechnen.

0. *Abgeschlossenheit:* Die Summe beliebiger Matrizen $\left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right), \left(\begin{smallmatrix} \tilde{x} & -\tilde{y} \\ \tilde{y} & \tilde{x} \end{smallmatrix}\right) \in \mathcal{C}$ liegt wieder in $\mathcal{C}$, denn
$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix} + \begin{pmatrix} \tilde{x} & -\tilde{y} \\ \tilde{y} & \tilde{x} \end{pmatrix} = \begin{pmatrix} x+\tilde{x} & -(y+\tilde{y}) \\ y+\tilde{y} & x+\tilde{x} \end{pmatrix}$$
ist von der geforderten Form.
1. *Neutrales Element:* Die Nullmatrix $\left(\begin{smallmatrix} 0 & -0 \\ 0 & 0 \end{smallmatrix}\right)$ liegt in $\mathcal{C}$ und ist linksneutral, da für alle $\left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right) \in \mathcal{C}$
$$\begin{pmatrix} 0 & -0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = \begin{pmatrix} 0+x & -(0+y) \\ 0+y & 0+x \end{pmatrix} = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$
2. *Assoziativität:* Für beliebige $M, \widetilde{M}, \widetilde{\widetilde{M}} \in \mathcal{C}$ gilt $(M+\widetilde{M})+\widetilde{\widetilde{M}} = M+(\widetilde{M}+\widetilde{\widetilde{M}})$, da allgemein die Matrizenaddition assoziativ ist.[1]
3. *Inverse Elemente:* Zu einer beliebigen Matrix $\left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right) \in \mathcal{C}$ liegt die Matrix $\left(\begin{smallmatrix} -x & -(-y) \\ -y & -x \end{smallmatrix}\right)$ in $\mathcal{C}$ und ist linksinvers:
$$\begin{pmatrix} -x & -(-y) \\ -y & -x \end{pmatrix} + \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = \begin{pmatrix} -x+x & -(-y+y) \\ -y+y & -x+x \end{pmatrix} = \begin{pmatrix} 0 & -0 \\ 0 & 0 \end{pmatrix}$$
4. *Kommutativität:* Für alle Matrizen $\left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right), \left(\begin{smallmatrix} \tilde{x} & -\tilde{y} \\ \tilde{y} & \tilde{x} \end{smallmatrix}\right) \in \mathcal{C}$ gilt
$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix} + \begin{pmatrix} \tilde{x} & -\tilde{y} \\ \tilde{y} & \tilde{x} \end{pmatrix} = \begin{pmatrix} x+\tilde{x} & -(y+\tilde{y}) \\ y+\tilde{y} & x+\tilde{x} \end{pmatrix} = \begin{pmatrix} \tilde{x}+x & -(\tilde{y}+y) \\ \tilde{y}+y & \tilde{x}+x \end{pmatrix} = \begin{pmatrix} \tilde{x} & -\tilde{y} \\ \tilde{y} & \tilde{x} \end{pmatrix} + \begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$

□

Behauptung (b)**.** *Bezüglich der Matrizenmultiplikation ist $\mathcal{C}$ keine Gruppe.*

Beweis. Wir müssen wieder die Gruppenaxiome prüfen.

0. *Abgeschlossenheit:* Das Produkt beliebiger Matrizen $\left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right), \left(\begin{smallmatrix} \tilde{x} & -\tilde{y} \\ \tilde{y} & \tilde{x} \end{smallmatrix}\right) \in \mathcal{C}$ liegt wieder in $\mathcal{C}$, denn
$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix} \begin{pmatrix} \tilde{x} & -\tilde{y} \\ \tilde{y} & \tilde{x} \end{pmatrix} = \begin{pmatrix} x\tilde{x}-y\tilde{y} & -(y\tilde{x}+x\tilde{y}) \\ y\tilde{x}+x\tilde{y} & x\tilde{x}-y\tilde{y} \end{pmatrix}$$
ist von der geforderten Form.

[1] Wenn man noch keinen Beweis dazu gesehen hat, kann man die Gleichheit auch nachrechnen.

1. *Neutrales Element:* Die Einheitsmatrix $\left(\begin{smallmatrix} 1 & -0 \\ 0 & 1 \end{smallmatrix}\right)$ liegt in $\mathcal{C}$ und ist linksneutral, da für alle $\left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right) \in \mathcal{C}$
$$\begin{pmatrix} 1 & -0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$
2. *Assoziativität:* Für beliebige $M, \widetilde{M}, \widetilde{\widetilde{M}} \in \mathcal{C}$ gilt $(M\widetilde{M})\widetilde{\widetilde{M}} = M(\widetilde{M}\widetilde{\widetilde{M}})$, da allgemein die Matrizenmultiplikation assoziativ ist.[1]
3. *Inverse Elemente:* Die Nullmatrix $\left(\begin{smallmatrix} 0 & -0 \\ 0 & 0 \end{smallmatrix}\right)$ besitzt kein Inverses, obwohl sie in $\mathcal{C}$ liegt. Das sieht man so: Wenn eine Matrix $\left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right) \in \mathcal{C}$ linksinvers zur Nullmatrix wäre, würde
$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix} \begin{pmatrix} 0 & -0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -0 \\ 0 & 1 \end{pmatrix}$$
gelten, was aber nicht stimmt. (Alternativ kann man auch bekanntes Lineare-Algebra-Wissen zitieren.)
4. *Kommutativität:* Für alle Matrizen $\left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right), \left(\begin{smallmatrix} \tilde{x} & -\tilde{y} \\ \tilde{y} & \tilde{x} \end{smallmatrix}\right) \in \mathcal{C}$ gilt
$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix} \begin{pmatrix} \tilde{x} & -\tilde{y} \\ \tilde{y} & \tilde{x} \end{pmatrix} = \begin{pmatrix} x\tilde{x} - y\tilde{y} & -(y\tilde{x} + x\tilde{y}) \\ y\tilde{x} + x\tilde{y} & x\tilde{x} - y\tilde{y} \end{pmatrix} = \begin{pmatrix} \tilde{x}x - \tilde{y}y & -(\tilde{y}x + \tilde{x}y) \\ \tilde{y}x + \tilde{x}y & \tilde{x}x - \tilde{y}y \end{pmatrix} = \begin{pmatrix} \tilde{x} & -\tilde{y} \\ \tilde{y} & \tilde{x} \end{pmatrix} \begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$

Zusammengenommen ist also $\mathcal{C}$ bezüglich der Matrizenmultiplikation keine Gruppe. Unsere Rechnungen zeigen aber, dass zumindest $\mathcal{C} \setminus \left\{\left(\begin{smallmatrix} 0 & -0 \\ 0 & 0 \end{smallmatrix}\right)\right\}$ eine Gruppe ist. Diese ist sogar abelsch, obwohl die Matrizenmultiplikation im Allgemeinen nicht kommutativ ist. □

Bezeichne $\mathbb{C} = \{a + \mathrm{i}b \mid a, b \in \mathbb{R}\}$ die Menge der komplexen Zahlen. Wir definieren die Abbildung
$$\begin{array}{rccc} F\colon & \mathbb{C} & \longrightarrow & \mathcal{C} \\ & a + \mathrm{i}b & \longmapsto & \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right). \end{array}$$

Behauptung (c1)**.** *Die Abbildung F ist $\mathbb{R}$-linear.*

Beweis. Hierzu sind zwei Aussagen zu zeigen:

1. Für beliebige Elemente $z = a + \mathrm{i}b, \tilde{z} = \tilde{a} + \mathrm{i}\tilde{b} \in \mathbb{C}$ gilt
$$F(z+\tilde{z}) = F((a+\tilde{a})+\mathrm{i}(b+\tilde{b})) = \begin{pmatrix} a+\tilde{a} & -(b+\tilde{b}) \\ b+\tilde{b} & a+\tilde{a} \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} \tilde{a} & -\tilde{b} \\ \tilde{b} & \tilde{a} \end{pmatrix} = F(z)+F(\tilde{z}).$$
2. Für jedes Element $z = a + \mathrm{i}b \in \mathbb{C}$ und für jede reelle Zahl $r \in \mathbb{R}$ gilt
$$F(rz) = F(ra + \mathrm{i}rb) = \begin{pmatrix} ra & -rb \\ rb & ra \end{pmatrix} = r \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = r\, F(z).$$ □

Behauptung (c2)**.** *Die Abbildung F ist multiplikationstreu.*

Beweis. Für beliebige Elemente $z = a + \mathrm{i}b, \tilde{z} = \tilde{a} + \mathrm{i}\tilde{b} \in \mathbb{C}$ gilt
$$F(z\tilde{z}) = F((a\tilde{a} - b\tilde{b}) + \mathrm{i}(b\tilde{a} + a\tilde{b})) = \begin{pmatrix} a\tilde{a} - b\tilde{b} & -(b\tilde{a} + a\tilde{b}) \\ b\tilde{a} + a\tilde{b} & a\tilde{a} - b\tilde{b} \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} \tilde{a} & -\tilde{b} \\ \tilde{b} & \tilde{a} \end{pmatrix} = F(z)\, F(\tilde{z}).$$
□

Blatt 4, Aufgabe 2

Bei dieser Aufgabe ging es darum, von vier gegebenen Abbildungen zu prüfen, ob sie linear sind. Am einfachsten geht das, indem man stur die Definition von Linearität nachrechnet. Hier folgt eine schwierigere, dafür schnellere Lösung.

Behauptung. *Die Abbildung* $A_1 \colon \mathbb{R}^3 \to \mathbb{R}^2, u \mapsto M_1 u$, *wobei* M_1 *die Matrix*

$$M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix} \in \mathbb{R}^{2\times 3}$$

bezeichnet, ist linear.

Beweis. Klar, da die Multiplikation mit einer festen Matrix stets linear ist. □

Behauptung. *Die Abbildung*

$$A_2 \colon \mathbb{R}^3 \longrightarrow \mathbb{R}^3, \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} x+1 \\ y+2 \\ z+3 \end{pmatrix}$$

ist nicht linear.

Beweis. Jede lineare Abbildung bildet den Nullvektor des Definitionsraums auf den Nullvektor des Zielraums ab. Die Abbildung A_2 tut das aber nicht, da $A_2(0) = (1,1,1)^T \neq 0$, und ist somit nicht linear. □

Behauptung. *Die Abbildung* $A_3 \colon \mathbb{R}^3 \to \mathbb{R}^3, u \mapsto M_3 u$, *wobei* M_3 *die Matrix*

$$M_3 = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix} \in \mathbb{R}^{3\times 3}$$

bezeichnet, ist linear.

Beweis. Klar, da die Multiplikation mit einer festen Matrix stets linear ist. □

Behauptung. *Die Abbildung* $A_4 := A_1 \circ A_3$ *ist linear.*

Beweis. Klar, da die Verkettung linearer Abbildungen stets linear ist. □

Die Matrix von A_4 ergibt sich übrigens als das Produkt der Matrizen von A_1 und A_3, ist also

$$M_1 M_3 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

Blatt 5, Aufgabe 2

Sei G eine Gruppe und für $g \in G$ die *Ordnung* $\operatorname{ord}(g)$ *von* g als die Anzahl der Elemente der Untergruppe $\langle g \rangle \subset G$ definiert.

Sei ein beliebiges $g \in G$ mit $\operatorname{ord}(g) < \infty$ gegeben.

Behauptung (a)**.** $\operatorname{ord}(g) = \min\{n \in \mathbb{N} \mid g^n = e\}$

Beweis. Da $\operatorname{ord}(g) < \infty$, kann die Liste

$$g^0, g^1, g^2, \ldots$$

nicht aus lauter verschiedenen Gruppenelementen bestehen. Also gibt es gewisse Exponenten i, j (oBdA $i > j$) mit $g^i = g^j$. Daraus folgt $g^{i-j} = e$. Damit existiert das Minimum der rechten Seite der Gleichung.

Sei nun n dieses Minimum, also die kleinste natürliche Zahl (≥ 1) mit $g^n = e$. Wir wollen zeigen, dass $n = \operatorname{ord}(g)$. Dazu erinnern wir uns an die Darstellung von $\langle g \rangle$ und vereinfachen diese:

$$\begin{aligned} \langle g \rangle &= \{\ldots, g^{-2}, g^{-1}, g^0, g^1, g^2, \ldots\} \\ &= \{g^0, g^1, g^2, \ldots\} \\ &= \{g^0, g^1, g^2, \ldots, g^{n-1}\} \end{aligned}$$

Dabei müssen wir die einzelnen Schritte begründen:

- Der erste Schritt folgt nach Blatt 4, Aufgabe 4(iii).
- Da $g^n = g\, g^{n-1} = e$, ist das Inverse von g das Gruppenelement g^{n-1}. Somit gilt $g^{-k} = g^{k(n-1)}$ für alle $k \geq 1$, womit wir die negativen g-Potenzen also nicht separat aufführen müssen, da sie jeweils gleich gewissen nichtnegativen g-Potenzen sind. Das begründet den zweiten Schritt.
- Da $g^n = e$, müssen wir g^n nicht separat aufführen. Da $g^{n+1} = g^n\, g = g$, müssen wir auch g^{n+1} nicht separat aufführen. Diese Argumentation können wir unbegrenzt fortführen, sodass wir also sehen, dass wir die Elemente g^k mit $k \geq n$ nicht aufführen müssen. Damit ist der dritte Schritt gezeigt.

Als Zwischenstand können wir festhalten: Die Anzahl der Elemente von $\langle g \rangle$ ist höchstens n. Um zu zeigen, dass sie genau n ist, müssen wir jetzt noch zeigen, dass in der Aufzählung $g^0, \ldots, g^{n-1}$ kein Element mehr als einmal vorkommt.

Sei dazu $g^i = g^j$ mit $i, j \in \{0, \ldots, n-1\}$, oBdA $i \geq j$. Dann folgt $g^{i-j} = e$. Wäre nun $i - j \neq 0$, so wäre $i - j$ eine natürliche Zahl, die kleiner als n ist, und trotzdem die Bedingung $g^{i-j} = e$ erfüllt. Das kann nicht sein, da n nach Definition die kleinste solcher Zahlen ist. □

Behauptung (b)**.** $g^n = e \Leftrightarrow \operatorname{ord}(g) \mid n$

Beweis. Sei eine beliebige ganze Zahl n gegeben. Diese können wir durch die Ordnung von g mit Rest teilen:

$$n = k \cdot \operatorname{ord}(g) + r,$$

für gewisse $k \in \mathbb{Z}$, $r \in \{0, \ldots, \operatorname{ord}(g) - 1\}$. Dann sehen wir:

$$g^n = g^{k \cdot \operatorname{ord}(g) + r} = (g^{\operatorname{ord}(g)})^k \, g^r = e^k \, g^r = g^r$$

Also ist $g^n = e$ genau dann, wenn $g^r = e$. Das ist wiederum genau dann der Fall, wenn $r = 0$ ist (nach dem Argument im letzten Absatz des vorigen Beweises). Schließlich gilt das genau dann, wenn n durch $\operatorname{ord}(g)$ teilbar ist. □

Behauptung (c)**.** $\langle g \rangle = \{g^0, g^1, g^2, \ldots, g^{n-1}\}$

Beweis. Das haben wir bereits in (a) bewiesen. □

Behauptung (d)**.** $\operatorname{ord}(g^k) = \operatorname{ord}(g) \,/\, \operatorname{ggT}(k, \operatorname{ord}(g))$

Beweis. Nach (a) ist die Ordnung von g^k der kleinste Exponent n derart, dass $(g^k)^n = g^{kn} = e$ ist. Also ist kn das kleinste gemeinsame Vielfache von k und $\operatorname{ord}(g)$, womit nach einer Formel der fünften Klasse

$$kn = k \cdot \operatorname{ord}(g) \,/\, \operatorname{ggT}(k, \operatorname{ord}(g))$$

gilt. Durch Kürzen sehen wir, dass $n = \operatorname{ord}(g) \,/\, \operatorname{ggT}(k, \operatorname{ord}(g))$. □

Blatt 5, Aufgabe 4(b)

Sei G eine Gruppe und $Z(G) := \{g \in G \mid gh = hg \text{ für alle } h \in G\} \subset G$.

Behauptung. *Die Teilmenge $Z(G)$ ist ein Normalteiler von G.*

Beweis. Zunächst müssen wir zeigen, dass $Z(G)$ eine Untergruppe von G ist:

1. Es gilt $e \in Z(G)$, denn $eh = he$ für alle $h \in G$.
2. Zu $g, \tilde{g} \in Z(G)$ liegt auch $g\tilde{g}$ in $Z(G)$, da $(g\tilde{g})h = gh\tilde{g} = h(g\tilde{g})$ für alle $h \in G$.
3. Zu $g \in Z(g)$ liegt auch g^{-1} in $Z(G)$, da $g^{-1}h = (h^{-1}g)^{-1} = (gh^{-1})^{-1} = hg^{-1}$ für alle $h \in G$.

Zum Nachweis der Normalteilereigenschaft sei nun ein beliebiges $g \in Z(g)$ und $h \in G$ gegeben. Dann liegt in der Tat $h^{-1}gh$ in $Z(g)$, denn $h^{-1}gh = h^{-1}hg = g$. □

Blatt 4, Aufgabe 4(c)

Behauptung. *Die Kerne der Gruppenhomomorphismen sind genau die Normalteiler.*

Beweis. Wir müssen zwei Teilaussagen zeigen:

1. Der Kern eines jeden Gruppenhomomorphismus ist ein Normalteiler.
2. Jeder Normalteiler ist der Kern irgendeines Gruppenhomomorphismus.

Zu 1.: Sei $\varphi\colon G \to H$ ein beliebiger Gruppenhomomorphismus. Dass $\ker\varphi$ eine Untergruppe von G ist, wurde schon in der Vorlesung gezeigt. Zum Nachweis der Normalteilereigenschaft sei ein beliebiges $u \in \ker\varphi$ und $g \in G$ gegeben. Dann liegt auch $g^{-1}ug$ in $\ker\varphi$, denn $\varphi(g^{-1}ug) = \varphi(g)^{-1}\,\varphi(u)\,\varphi(g) = \varphi(g)^{-1}\,e\,\varphi(g) = e$.

Zu 2.: Sei G irgendeine Gruppe und N irgendein Normalteiler von G. Dann gibt es (nach Vorlesung) die Quotientengruppe G/N und die kanonische Projektionsabbildung $\pi\colon G \to G/N, g \mapsto [g]$. Aus der Vorlesung wissen wir, dass der Kern dieser Abbildung gerade N ist. □

Blatt 5, Aufgabe 5

Sei G eine Gruppe, U eine Untergruppe und N ein Normalteiler von G. Außerdem gelte $N \subset U$.

Zur Erinnerung: Die Elemente von U/N sind Äquivalenzklassen von Elementen aus U bzgl. der Äquivalenzrelation $u \sim v :\Leftrightarrow u^{-1}v \in N$. Die zu $u \in U$ gehörige Äquivalenzklasse schreibt man als $[u] \in U/N$ und aus der Vorlesung ist bekannt, dass $[u] = uN := \{un \,|\, n \in N\}$ gilt.

Ferner wurde in der Vorlesung gezeigt, dass U/N eine Gruppe wird, wenn man $uN \cdot vN := (uv)N$ für $uN, vN \in U/N$ definiert und wenn N ein Normalteiler von U ist.

Behauptung (a1)**.** *N ist ein Normalteiler von U.*

Beweis. Klar ist, dass N die Untergruppenaxiome bezüglich U als Obergruppe erfüllt: Denn N erfüllt die Untergruppenaxiome bezüglich G als Obergruppe, und die Verknüpfung, das neutrale Element und die inversen Elemente von U sind dieselben wie die von G.

Zum Nachweis der Normalteilereigenschaft seien $n \in N$ und $u \in U$ beliebig gegeben. Dann liegt in der Tat $u^{-1}\,n\,u$ in N, da $u \in G$ und N ein Normalteiler in G ist. □

Behauptung (a2)**.** *U/N ist eine Untergruppe von G/N.*

Beweis. Zunächst zeigen wir, dass U/N eine Teilmenge von G/N ist (das ist nämlich nicht offensichtlich). Sei also ein beliebiges Element x aus U/N gegeben. Dieses muss von der Form $x = uN$ sein, wobei u ein Element aus U ist. Also gilt auch $x \in G/N$.

Nun zeigen wir, dass die Gruppenverknüpfung auf U/N die Einschränkung der Verknüpfung auf G/N ist. Seien also $x, y \in U/N$ beliebig gegeben. Dann gibt es $u, v \in U$ mit $x = uN, y = vN$. Das Produkt von x und y in der Gruppe U/N ist dann definitionsgemäß $(xy)N$. Das Produkt von x und y in der Gruppe G/N ist nach Definition ebenfalls $(xy)N$, also stimmen die beiden Produkte überein. □

Sei nun auch U ein Normalteiler von G.

Behauptung (b1)**.** *U/N ist ein Normalteiler von G/N.*

Beweis. Dass U/N eine Untergruppe von G/N ist, haben wir eben schon gesehen. Seien jetzt zum Nachweis der Normalteilereigenschaft $[u] \in U/N$ und $[g] \in G/N$ beliebig gegeben. Dann liegt $[g]^{-1}\,[u]\,[g] = [g^{-1}ug]$ in der Tat in U/N, da $g^{-1}ug \in U$, da U ein Normalteiler von G ist. □

Folglich ist $(G/N)/(U/N)$ eine Gruppe.

Behauptung (b2)**.** *Die Gruppen G/U und $(G/N)/(U/N)$ sind zueinander isomorph (d. h. es gibt einen bijektiven Gruppenhomomorphismus zwischen den beiden Gruppen).*

Beweis. Dazu gibt es zwei Varianten, ohne und mit Homomorphiesatz.

Ohne Homomorphiesatz. Wir geben direkt den gesuchten Gruppenisomorphismus an:

$$\begin{array}{rccc} \psi\colon & G/U & \longrightarrow & (G/N)/(U/N) \\ & [g]_U & \longmapsto & [\,[g]_N\,]_{U/N} \end{array}$$

Die einzelnen Symbole haben dabei folgende Bedeutung:

- Zu $g \in G$ bezeichnet $[g]_U$ die Äquivalenzklasse von g in der Gruppe G/U, es gilt also $[g]_U = gU$.
- Zu $g \in G$ bezeichnet $[g]_N$ die Äquivalenzklasse von g in der Gruppe G/N, also $[g]_N = gN$.
- Zu $p \in G/N$ bezeichnet $[p]_{U/N}$ die Äquivalenzklasse von p in der Gruppe $(G/N)/(U/N)$, also $[p]_{G/N} = p\,(U/N)$.

Wir müssen zeigen, dass ψ wohldefiniert, bijektiv und ein Gruppenhomomorphismus ist.

1. Zur Wohldefiniertheit: Gelte $g \sim_U g'$ für $g, g' \in G$, also $g^{-1}g' \in U$. Dann gilt auch $[g]_N \sim_{U/N} [g']_N$, denn $([g]_N)^{-1}[g']_N = [g^{-1}g']_N \in U/N$.
2. Zur Injektivität: Seien $[g]_U, [g']_U \in G/U$ mit $\psi([g]) = \psi([g'])$ gegeben. Dann gilt also $([g]_N)^{-1}[g']_N = [g^{-1}g'] \in U/N$, also liegt $g^{-1}g'$ in U. Damit folgt $[g]_U = [g']_U$.
3. Zur Surjektivität: Sei ein $y \in (G/N)/(U/N)$ beliebig gegeben. Dann gibt es ein $p \in G/N$ mit $y = [p]_{U/N}$. Ferner gibt es zu p ein $g \in G$ mit $p = [g]_N$. Also gilt für $x := [g] \in G/U$, dass $\psi(x) = [\,[g]_N\,]_{U/N} = y$.
4. Zur Homomorphieeigenschaft: Seien $[g]_U, [g']_U \in G/U$ beliebig gegeben. Dann gilt

$$\begin{aligned} \psi([g]_U \cdot [g']_U) &= \psi([gg']_U) = [\,[gg']_N\,]_{U/N} \\ &= [\,[g]_N \cdot [g']_N\,]_{U/N} = [\,[g]_N\,]_{U/N} \cdot [\,[g']_N\,]_{U/N} \\ &= \psi([g]_U) \cdot \psi([g']_U). \end{aligned}$$

Mit Homomorphiesatz. Wir definieren

$$\begin{array}{rccc} \theta\colon & G & \longrightarrow & (G/N)/(U/N) \\ & g & \longmapsto & [\,[g]_N\,]_{U/N}. \end{array}$$

Dann kann man nachrechnen, dass θ ein surjektiver Gruppenhomomorphismus mit $\ker\theta = U$ ist. Nach dem Homomorphiesatz ist dann

$$\begin{array}{rccc} \bar{\theta}\colon & G/U & \longrightarrow & (G/N)/(U/N) \\ & [g]_U & \longmapsto & \theta(g) = [\,[g]_N\,]_{U/N} \end{array}$$

ein Gruppenisomorphismus. □

Bemerkung. Der Isomorphismus aus dem Homomorphiesatz stimmt also mit dem explizit angegebenen Gruppenisomorphismus überein. Außerdem sind die Nachweise, die man in den beiden Beweisvarianten erbringen muss, gleich viele und etwa gleich schwer.

Blatt 6, Aufgabe 4

Sei $\mathbb{Z}[\mathrm{i}] := \{f(\mathrm{i}) \mid f \in \mathbb{Z}[X]\} \subset \mathbb{C}$, wobei $\mathrm{i} \in \mathbb{C}$ die imaginäre Einheit bezeichne.

Behauptung (a)**.** $\mathbb{Z}[\mathrm{i}] = \{u + \mathrm{i}v \mid u, v \in \mathbb{Z}\}$.

Beweis. Für die Richtung „$\supset$“ seien $u, v \in \mathbb{Z}$ beliebig gegeben. Für $f := u + vX \in \mathbb{Z}[X]$ gilt dann $u + \mathrm{i}v = f(\mathrm{i})$, also liegt $u + \mathrm{i}v$ in der Tat in $\mathbb{Z}[\mathrm{i}]$.

Für die Richtung „$\subset$“ sei $f \in \mathbb{Z}[X]$ beliebig gegeben. Die komplexe Zahl $f(\mathrm{i})$ ist dann also eine Linearkombination der Zahlen $\mathrm{i}^0, \mathrm{i}^1, \mathrm{i}^2, \mathrm{i}^3, \ldots$ mit ganzzahligen Koeffizienten. Jede dieser Zahlen liegt in der rechten Menge:

$$\begin{aligned}
\mathrm{i}^0 = \mathrm{i}^4 = \mathrm{i}^8 &= \mathrm{i}^{12} = \cdots = \quad 1 + \mathrm{i} \cdot 0 \\
\mathrm{i}^1 = \mathrm{i}^5 = \mathrm{i}^9 &= \mathrm{i}^{13} = \cdots = \quad 0 + \mathrm{i} \cdot 1 \\
\mathrm{i}^2 = \mathrm{i}^6 = \mathrm{i}^{10} = \mathrm{i}^{14} &= \cdots = -1 + \mathrm{i} \cdot 0 \\
\mathrm{i}^3 = \mathrm{i}^7 = \mathrm{i}^{11} = \mathrm{i}^{15} &= \cdots = \quad 0 + \mathrm{i} \cdot (-1)
\end{aligned}$$

Damit liegt auch $f(\mathrm{i})$ in der rechten Menge. □

Sei die Funktion

$$\begin{array}{rccc} \varphi\colon & \mathbb{Z}[\mathrm{i}] \setminus \{0\} & \longrightarrow & \mathbb{N}_0, \\ & z & \longmapsto & |z|^2, \end{array}$$

definiert, wobei die Betragsstriche den komplexen Betrag bezeichnen (also $\varphi(u + \mathrm{i}v) = (\sqrt{u^2 + v^2})^2 = u^2 + v^2$ für $u, v \in \mathbb{Z}$).

Behauptung (b)**.** *Der Ring* $\mathbb{Z}[\mathrm{i}]$ *ist vermöge* φ *ein euklidischer Ring.*

Beweis. Dazu müssen wir die Teilaussagen (e1) und (e2) der Aufgabenstellung zeigen:

1. Seien $a, b \in \mathbb{Z}[\mathrm{i}]$ mit $ab \neq 0$. Dann ist insbesondere b nicht null und es gilt $\varphi(b) = |b|^2 \geq 1$. Somit folgt $\varphi(ab) = |ab|^2 = |a|^2|b|^2 \geq |a|^2 = \varphi(a)$.
2. Seien $a, b \in \mathbb{Z}[\mathrm{i}]$ mit $b \neq 0$. Dann ist der Quotient $x := a/b$ eine gewisse komplexe Zahl. Sei u der Real- und v der Imaginärteil von x, d. h. gelte $x = u + \mathrm{i}v$ mit $u, v \in \mathbb{R}$.

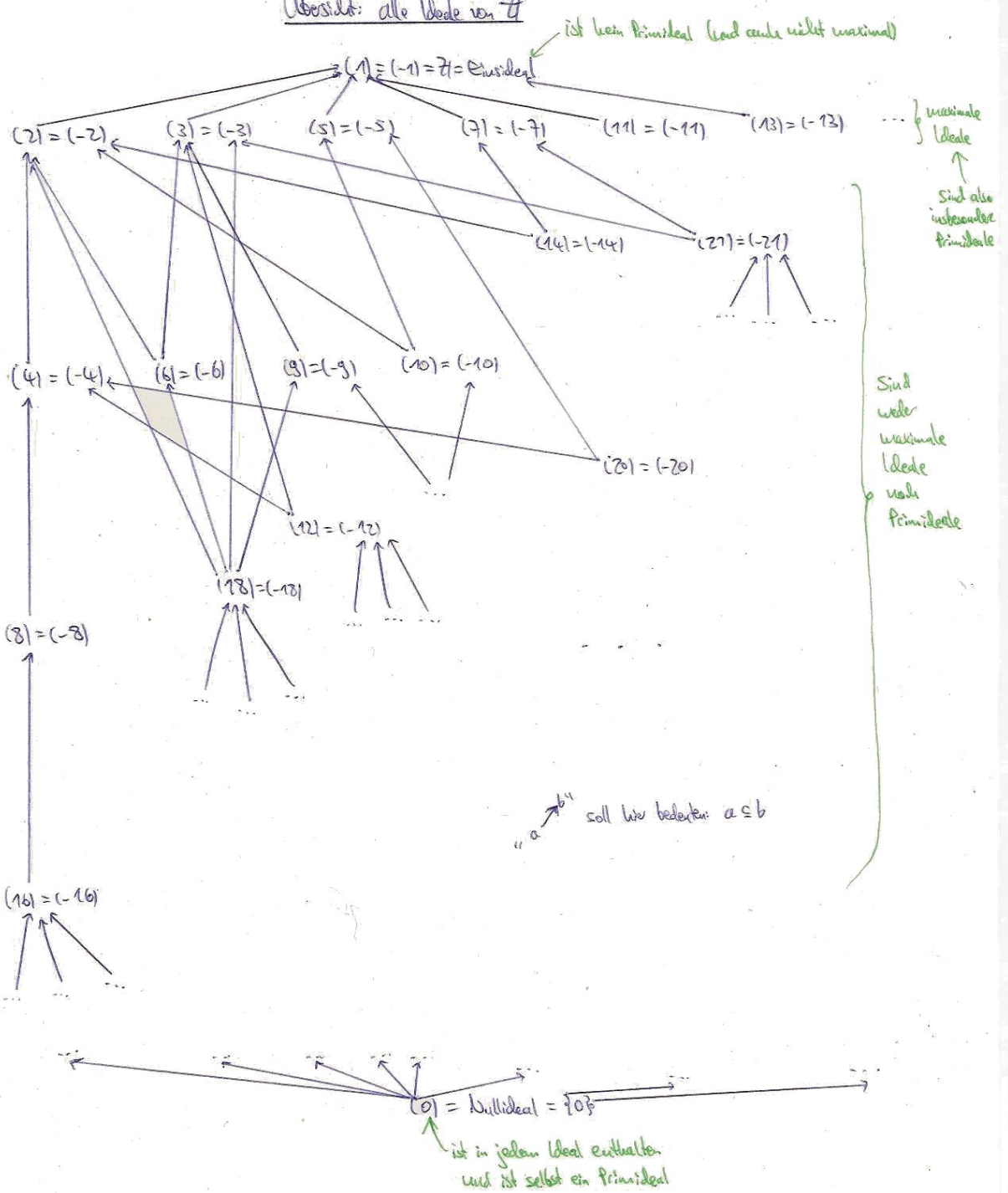
   Wir wählen nun ganzzahlige Näherungen $\tilde{u}, \tilde{v} \in \mathbb{Z}$ von u bzw. v, also ganze Zahlen mit $|u - \tilde{u}|, |v - \tilde{v}| \leq \frac{1}{2}$, und setzen $q := \tilde{u} + \mathrm{i}\tilde{v} \in \mathbb{Z}[\mathrm{i}]$, $r := a - qb$.

   Dann ist entweder der Rest r null (das passiert genau dann, wenn u und v selbst schon ganzzahlig waren), oder er ist nicht null; dann gilt die Abschätzung

$$\begin{aligned}
\varphi(r) = |a - qb|^2 = |b(x - q)|^2 &= |b|^2 \cdot ((u - \tilde{u})^2 + (v - \tilde{v})^2) \\
&\leq |b|^2 \cdot (\tfrac{1}{4} + \tfrac{1}{4}) = \tfrac{1}{2}\varphi(b) < \varphi(b).
\end{aligned}$$

□

Übersicht: alle Ideale von $\mathbb{Z}$



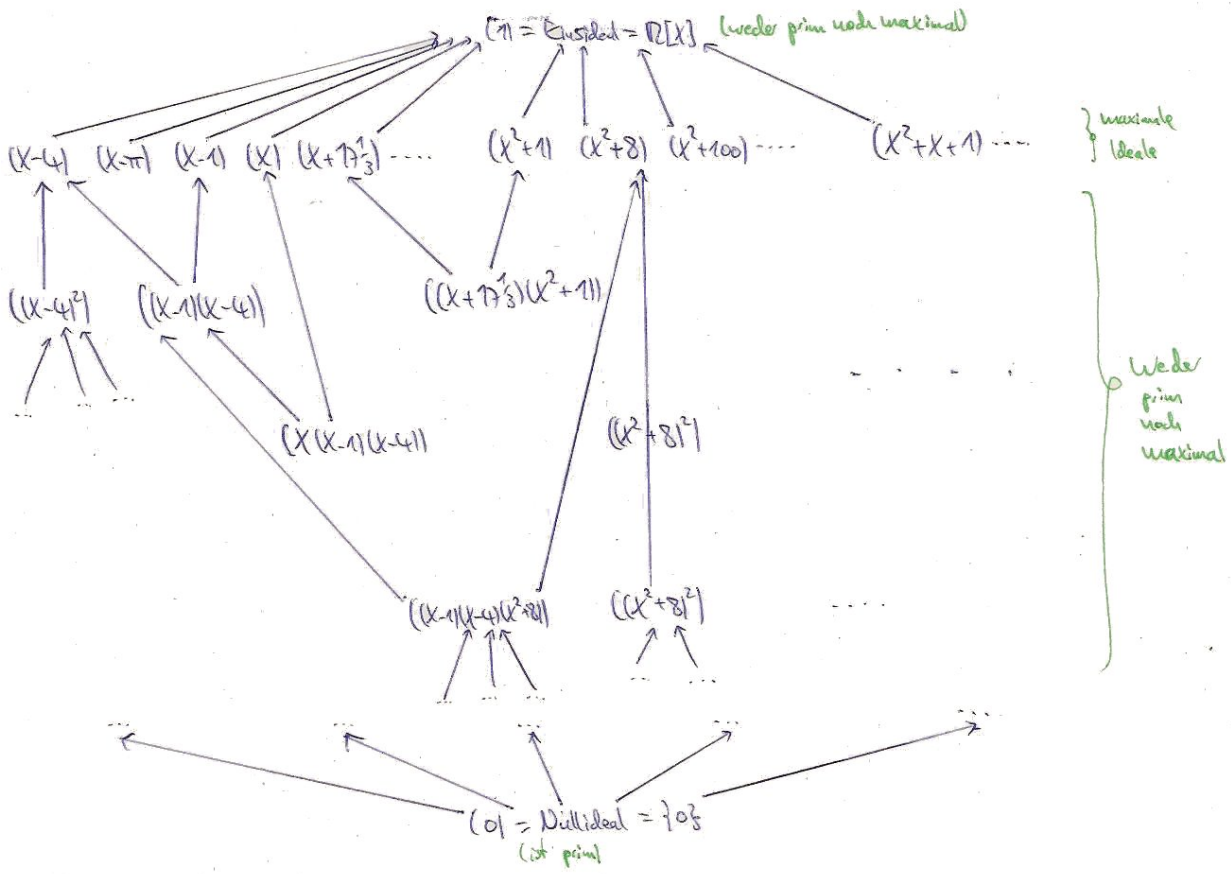
Bem.: $(n) =$ „von n erzeugtes Ideal" $= \text{Menge aller ganzzahligen Vielfachen von } n = n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$

Bem.: Für Ideale in $\mathbb{Z}$ gilt: $(n) + (m) = (ggT(n,m))$, $(n) \cap (m) = (kgV(n,m))$

Summe von Idealen, allgemein definiert als $a + b = \{x + y \mid x \in a, y \in b\}$

Schnitt von Idealen, allgemein definiert als $a \cap b := \{x \in R \mid x \in a \text{ und } x \in b\}$

Übersicht alle Ideale von $\mathbb{R}[X]$



Bem: $(X-4)$ = Menge alle $\mathbb{R}[X]$-Vielfachen von $(X-4) = (\frac{1}{7}(X-4)) = (4-X) = (\frac{e}{\pi}(X-4)) = \dots$

Bem: Für Ideale in $\mathbb{R}[X]$ gilt: $(f)+(g) = (ggT(f,g))$, $(f)\cap(g) = (kgV(f,g))$.

Zum Beispiel: $(X-2)+(X-3) = (1)$.

$(X-5)\cap(X-5) = (X-5)$

$(X-5)\cap(X-6) = ((X-5)(X-6))$

Übersicht: alle Ideale von K

irgendein Körper, z.B. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{5}, i), \ldots$

$(1) = R$ Einsideal
(wieder maximal noch prim)
↑
$(0) = R$ Nullideal
(maximal, insbesondere prim)

andere Ideale gibt es nicht!

Übersicht: alle Ideale des Nullrings

$(0) = (1)$
$= R$ Einsideal
$= R$ Nullideal
(weder maximal noch prim)

andere Ideale gibt es nicht!

Rechenregeln für Ideale

1. $(x_1, \ldots, x_n) + (y_1, \ldots, y_m) = (x_1, \ldots, x_n, y_1, \ldots, y_m)$
2. $(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_m) = (x_1y_1, \ldots, x_1y_m, x_2y_1, \ldots, x_2y_m, \ldots\ldots, x_ny_1, \ldots, x_ny_m)$
3. Die Reihenfolge der Erzeuger spielt keine Rolle.
4. Ein Ideal ändert sich nicht, wenn man zu einem Erzeuger ein beliebiges Vielfaches eines anderen Erzeugers addiert.
5. Ist ein Erzeuger ein Vielfaches eines anderen, so kann man ihn weglassen.
6. Ein Ideal ändert sich nicht, wenn man einen Erzeuger mit einer beliebigen Einheit multipliziert.

   Ist einer der Erzeuger eine Einheit, so ist das Ideal schon das Einsideal.
7. Speziell in Hauptidealringen:

$$(x_1, \ldots, x_n) = (\mathrm{ggT}(x_1, \ldots, x_n))$$
$$(x) \cap (y) = (\mathrm{kgV}(x, y))$$

8. Speziell in Polynomringen:

$$(f_1(X), \ldots, f_n(X), X - a) = (f_1(a), \ldots, f_n(a), X - a)$$

Beispiele

- in $\mathbb{Z}$: $(8, 6, 4) = (\mathrm{ggT}(8, 6, 4)) = (2)$
- in $\mathbb{Z}$: $(2, 4) \cdot (3, 6) = (2 \cdot 3, 2 \cdot 6, 4 \cdot 3, 4 \cdot 6) = (6, 12, 12, 24) = (6)$
- in $\mathbb{Z}[X]$: $(X^2 - 25, X - 3) = (3^2 - 25, X - 3) = (-16, X - 3) = (16, X - 3)$
- in $\mathbb{Q}$: $(8, 6, 4) = (1) = (2) = (3173)$
- in $\mathbb{R}[X]$: $(X^2 - 25, X - 3) = (3^2 - 25, X - 3) = (-16, X - 3) = (1)$

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 $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$ und

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

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 maxial 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.

Rechenregeln für Körpererweiterungen

Folgende Regeln kann man benutzen, um Darstellungen von Körpererweiterungen der Form $L = K(x_1, \ldots, x_n)$ über K zu vereinfachen:

a) Die Reihenfolge der Erzeuger spielt keine Rolle.

b) Erzeuger, die in K liegen, kann man weglassen.

c) Man kann beliebige Elemente aus K zu Erzeugern addieren und subtrahieren, sowie (falls nicht null) multiplizieren und dividieren.

d) Man kann beliebige K-Vielfache eines Erzeugers auf einen anderen addieren und subtrahieren, sowieso (falls nicht null) multiplizieren und dividieren.

Außerdem helfen folgende Tatsachen (F beliebiger Körper):

e) $K(x_1, \ldots, x_n)(y_1, \ldots, y_m) = K(x_1, \ldots, x_n, y_1, \ldots, y_m)$

f) $K(x_1, \ldots, x_n) \subseteq F$ genau dann, wenn $K \subseteq F$ und $x_1, \ldots, x_n \in F$.

Im Allgemeinen gilt nicht, dass $K(x, y) = K(x + y)$.

Beispiele

1. $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$
2. $\mathbb{Q}(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}) = \mathbb{Q}(1 + \sqrt{5}, 1 - \sqrt{5}) = \mathbb{Q}(\sqrt{5}, -\sqrt{5}) = \mathbb{Q}(\sqrt{5})$
3. $\mathbb{Q}(\zeta^0, \zeta^1, \ldots, \zeta^5) = \mathbb{Q}(\zeta) = \mathbb{Q}(1 + \sqrt{3}\,\mathrm{i}) = \mathbb{Q}(\sqrt{3}\,\mathrm{i})$,
   für $\zeta := e^{2\pi\mathrm{i}/6} = \cos 60° + \mathrm{i} \sin 60° = \frac{1}{2}(1 + \sqrt{3}\,\mathrm{i})$.
4. $\mathbb{Q}(\sqrt{3})(\zeta^0, \ldots, \zeta^5) = \mathbb{Q}(\sqrt{3})(\sqrt{3}\,\mathrm{i}) = \mathbb{Q}(\sqrt{3}, \sqrt{3}\,\mathrm{i}) = \mathbb{Q}(\sqrt{3}, \mathrm{i})$,
   für ζ wie in Beispiel 3.
5. $\mathbb{Q}(\sqrt[8]{2}\,\zeta^0, \ldots, \sqrt[8]{2}\,\zeta^7) = \mathbb{Q}(\sqrt[8]{2}, \zeta, \zeta^2, \ldots, \zeta^7) = \mathbb{Q}(\sqrt[8]{2}, \zeta) = \mathbb{Q}(\sqrt[8]{2}, 1 + \mathrm{i}) = \mathbb{Q}(\sqrt[8]{2}, \mathrm{i})$,
   für $\zeta := e^{2\pi\mathrm{i}/8} = \frac{1}{\sqrt{2}}(1 + \mathrm{i})$.
6. $\mathbb{Q}(\text{alle sechs Nullstellen von } (X^4 - 2)(X^2 + 1)) = \mathbb{Q}(\sqrt[4]{2}, \mathrm{i})$
7. $\mathbb{Q}(\sqrt{2}, \mathrm{i}) = \mathbb{Q}(\sqrt{2} + \mathrm{i})$ (ein Ausnahmefall; knifflig)

Anwendungen

Die Darstellung zu vereinfachen ist hilfreich, wenn man...

– ... den Grad einer Körpererweiterung bestimmen möchte.

  Bsp.: Die Erweiterung von Beispiel 3 hat über $\mathbb{Q}$ den Grad 2, denn das Minimalpolynom von $\sqrt{3}\,\mathrm{i}$ über $\mathbb{Q}$ ist X^2+3 (wieso?). In der Ausgangsformulierung $\mathbb{Q}(\zeta^0, \zeta^1, \ldots, \zeta^5)$ erkennt man den Grad dagegen nicht so schnell.

– ... Zerfällungskörper in knapper Form angeben möchte.

– ... Galoisgruppen bestimmen möchte.

Kurzaufgaben zur Ringtheorie

. . . zu Beispielen für Ringe

Finde ein Beispiel für einen Ring, der. . .

1. . . . genau ein Ideal besitzt.
2. . . . genau zwei Ideale besitzt.
3. . . . keinen Nullteiler besitzt.
4. . . . genau einen Nullteiler besitzt.
5. . . . nur invertierbare Elemente enthält.

. . . zu Isomorphismen von Ringen

Seien R und S Ringe (kommutativ und mit Eins). Finde (mit Beweis) einen Isomorphismus zwischen. . .

1. . . . dem Faktorring $R/(0)$ und R selbst.
2. . . . dem Faktorring $R/(1)$ und dem Nullring.
3. . . . den Ringen $R \times S$ und $S \times R$.

. . . zu Idealeigenschaften

Sei R ein Ring (kommutativ und mit Eins). Zeige:

1. Genau dann ist R ein Integritätsbereich, wenn sein Nullideal ein Primideal ist.
2. Genau dann ist R ein Körper, wenn sein Nullideal ein maximales Ideal ist.

. . . zum Rechnen mit Idealen

Vereinfache folgende Ideale so weit wie möglich!

1. in $\mathbb{Z}$: $(9, 4, 101)$
2. in $\mathbb{Z}[X]$: $((X-2)(X-3), X-3)$
3. in $\mathbb{Z}[X]$: (X^3-2, X^4+1, X)
4. in $\mathbb{R}[X]$: $(15\,(X-3), 37\,(X^2-7X+12), 0)$

Kurzaufgaben zur Körpertheorie

1. Was ist das Minimalpolynom von $\sqrt{7}$ über $\mathbb{Q}$?
2. Was ist das Minimalpolynom von $\sqrt{9}$ über $\mathbb{Q}$?
3. Was ist das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}(\sqrt{2})$?

4. Welchen Grad hat $\mathbb{Q}(\sqrt{7})$ über $\mathbb{Q}$?
5. Welchen Grad hat $\mathbb{Q}(\sqrt{2},\sqrt{3})$ über $\mathbb{Q}(\sqrt{2})$?
6. Welchen Grad hat $\mathbb{Q}(\sqrt{2},\sqrt{3})$ über $\mathbb{Q}$?

7. Was ist eine $\mathbb{Q}(\sqrt{2})$-Basis von $\mathbb{Q}(\sqrt{2},\sqrt{3})$?
8. Was ist eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{2},\sqrt{3})$?

9. Ist die imaginäre Einheit i in $\mathbb{Q}(\sqrt{2})$ enthalten?
10. Ist $\sqrt{3}$ in $\mathbb{Q}(\sqrt{2})$ enthalten?
11. Zeige: $\mathbb{Q}(\sqrt{2},\mathrm{i}) = \mathbb{Q}(\sqrt{2}+\mathrm{i})$.
    Tipp: Zeige dazu, dass zum einen $\sqrt{2}$ und i in $\mathbb{Q}(\sqrt{2}+\mathrm{i})$ enthalten sind (was ist $(\sqrt{2}+\mathrm{i})^2$ und $(\sqrt{2}+\mathrm{i})^3$?) und zum anderen $\sqrt{2}+\mathrm{i}$ in $\mathbb{Q}(\sqrt{2},\mathrm{i})$ liegt.
    Warnung: Das Ergebnis dieser Aufgabe ist nicht allgemeingültig und nicht auf andere Fälle übertragbar.

12. Finde Beispiele für zwei über $\mathbb{Q}$ algebraische Zahlen $x, y \in \mathbb{C}$, sodass die Summe $x+y$ größeren, gleichen oder kleineren Grad über $\mathbb{Q}$ als x hat.

Aufgaben zur Idealtheorie

1. Seien $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale. Wieso ist die Teilmenge

$$\{xy \mid x \in \mathfrak{a}, y \in \mathfrak{b}\} \subseteq R$$

im Allgemeinen kein Ideal?

Tipp: Ein Gegenbeispiel genügt.

2. *Zeige:* Das Ideal $(X, Y) \subseteq R[X, Y]$ ist kein Hauptideal, wenn R ein beliebiger Integritätsbereich ist.

3. In der Vorlesung wurde gezeigt, dass das Ideal $(2, \omega) \subseteq \mathbb{Z}[\omega]$ mit

$$\omega := \frac{1 + \sqrt{-23}}{2}$$

ein Primideal ist; also ist $\mathbb{Z}[\omega]/(2, \omega)$ ein Integritätsbereich. Wir wollen eine möglichst einfache Darstellung dieses Rings herleiten. Die folgenden Teilaufgaben können unabhängig voneinander bearbeitet werden.

a) Was ist das Minimalpolynom von ω über $\mathbb{Q}$?

(Zum Weiterrechnen: $m_\omega = X^2 - X + 6 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$.)

b) *Zeige:* Der Kern des Ringhomomorphismus

$$\begin{array}{rccc} \mathrm{ev}_\omega\colon & \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}[\omega] \\ & f & \longmapsto & f(\omega) \end{array}$$

ist das Ideal $(m_\omega) \subseteq \mathbb{Z}[X]$.

Tipp für „⊆“: Sind in einer Polynomgleichung $f = gh$ mit $f, g, h \in \mathbb{Q}[X]$ die Polynome f und g ganzzahlig, und ist außerdem g primitiv, so ist auch h ganzzahlig.

c) Folgere mit dem Homomorphiesatz: $\mathbb{Z}[X]/(X^2 - X + 6) \cong \mathbb{Z}[\omega]$.

d) Vereinfache mithilfe der Rechenregeln für Ideale, wichtigen Ringisomorphismen und c) die Angabe des Faktorrings $\mathbb{Z}[\omega]/(2, \omega)$.

4. Prüfe nach demselben Muster, ob das Ideal $(3, \alpha) \subseteq \mathbb{Z}[\alpha]$, wobei

$$\alpha := \frac{1 + \sqrt{-7}}{2},$$

ein maximales Ideal ist.

Hauptsatz der Galoistheorie

Sei $L|K$ eine endliche, separable und normale Körpererweiterung. Sei $G := \mathrm{Gal}(L|K)$. Dann ist die Zuordnung

$$\begin{aligned}(\text{Menge der Untergruppen von } G) &\longrightarrow (\text{Menge der Zwischenerweiterungen von } L|K)\\ U &\longmapsto L^U := \{x \in L \,|\, \sigma(x) = x \text{ für alle } \sigma \in U\}\\ \{\sigma \in G \,|\, \sigma|_E = \mathrm{id}\} = \mathrm{Gal}(L|E) &\longmapsfrom E\end{aligned}$$

eine Bijektion. Genauer gilt für alle Zwischenerweiterungen E, E' von $L|K$ und Untergruppen U, U' von G:

1. $L^{\mathrm{Gal}(L|E)} = E$, $\qquad \mathrm{Gal}(L|L^U) = U$
2. $E \subseteq E' \Leftrightarrow \mathrm{Gal}(L|E) \supseteq \mathrm{Gal}(L|E')$, $\qquad U \subseteq U' \Leftrightarrow L^U \supseteq L^{U'}$
3. $|U| = [L : L^U]$, $\qquad [L^U : K] = |G|/|U|$
4. U Normalteiler von $G \Leftrightarrow L^U|K$ normale Erweiterung

   Wenn eine dieser beiden äquivalenten Bedingungen erfüllt ist, gilt: Die kanonische Abbildung
   $$\begin{array}{rcl}\mathrm{Gal}(L|K)\,/\,U & \longrightarrow & \mathrm{Gal}(L^U|K)\\ [\sigma] & \longmapsto & \sigma|_{L^U}\end{array}$$
   ein Gruppenisomorphismus.

Beispiel

Sei $L := \mathbb{Q}(\sqrt{2}, \mathrm{i})$ der Zerfällungskörper von $(X^2 - 2)(X^2 + 1)$ über $K := \mathbb{Q}$.

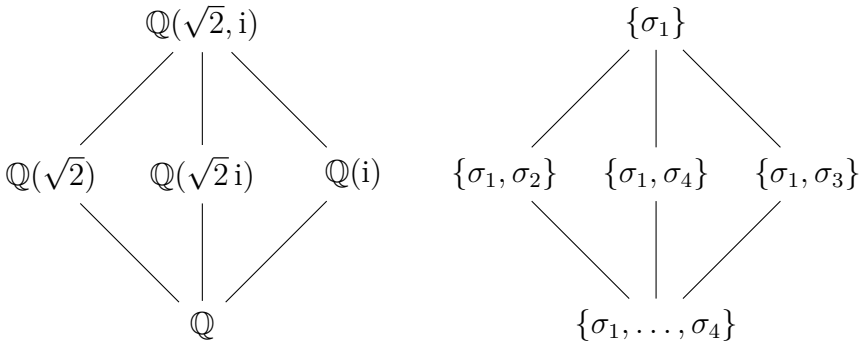
1. Die Galoisgruppe G besteht aus folgenden vier Elementen $\sigma_1, \ldots, \sigma_4$:
   $$\begin{aligned}\sigma_1{:}\sqrt{2} &\mapsto \sqrt{2}, & \mathrm{i} &\mapsto \mathrm{i}\\ \sigma_2{:}\sqrt{2} &\mapsto \sqrt{2}, & \mathrm{i} &\mapsto -\mathrm{i}\\ \sigma_3{:}\sqrt{2} &\mapsto -\sqrt{2}, & \mathrm{i} &\mapsto \mathrm{i}\\ \sigma_4{:}\sqrt{2} &\mapsto -\sqrt{2}, & \mathrm{i} &\mapsto -\mathrm{i}\end{aligned}$$

2. Die Verknüpfungstafel ist:

$\circ$	σ_1	σ_2	σ_3	σ_4
σ_1	σ_1	σ_2	σ_3	σ_4
σ_2	σ_2	σ_1	σ_4	σ_3
σ_3	σ_3	σ_4	σ_1	σ_2
σ_4	σ_4	σ_3	σ_2	σ_1

   Dazu sind die Nebenrechnungen $\sigma_2 \circ \sigma_2 = \sigma_1$ und $\sigma_3 \circ \sigma_3 = \sigma_1$ erforderlich, den Rest kann man nach der Regel „in jeder Zeile und Spalte muss jedes Gruppenelement genau einmal vorkommen“ erschließen.

3. Tafel der Untergruppen von G und der Zwischenerweiterungen von $\mathbb{Q}(\sqrt{2}, \mathrm{i})$ über $\mathbb{Q}$:



Im linken Diagramm steht oben die größte und unten die kleinste Zwischenerweiterung, im rechten Diagramm umgekehrt oben die kleinste und unten die größte Untergruppe der Galoisgruppe. Das ist so gemacht, dass zu einer Zwischenerweiterung an der entsprechenden Stelle rechts die zugehörige relative Galoisgruppe und zu einer Untergruppe entsprechend links der zugehörige Fixkörper steht.

4. Exemplarisch der Nachweis, dass $L^{\{\sigma_1,\sigma_4\}} = \mathbb{Q}(\sqrt{2}\,\mathrm{i})$:

   Die Richtung „$\supseteq$“ ist klar, da die Zahl $\sqrt{2}\,\mathrm{i}$ von σ_4 (und von σ_1 sowieso) festgehalten wird:

$$\sigma_4(\sqrt{2}\,\mathrm{i}) = \sigma_4(\sqrt{2})\,\sigma_4(\mathrm{i}) = (-\sqrt{2})(-\mathrm{i}) = \sqrt{2}\,\mathrm{i}$$

   Die andere Richtung folgt aus Gradgründen:

$$[L^{\{\sigma_1,\sigma_4\}} : \mathbb{Q}] = |G| \,/\, |\{\sigma_1, \sigma_4\}| = 4/2 = 2$$
$$[\mathbb{Q}(\sqrt{2}\,\mathrm{i}) : \mathbb{Q}] = 2$$

Zum Satz über das primitive Element

Der abstrakte Satz lautet:

Satz. *Sei $L|K$ eine endliche und separable Körpererweiterung. Dann gibt es ein sog.* primitives Element $z \in L$ *mit*

$$L = K(z).$$

Dass dieser Satz stimmt, ist sehr erstaunlich: Wenn die Voraussetzungen erfüllt sind, kann man also gegebene Erzeuger einer Körpererweiterung stets durch ein einzelnes bestimmtes Element ersetzen.

Beispiele:

1. Da $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$, ist $\sqrt{2}$ ein primitives Element für die Körpererweiterung $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) \mid \mathbb{Q}$.
2. Da $\mathbb{Q}(\sqrt{2}, \mathrm{i}) = \mathbb{Q}(\sqrt{2} + \mathrm{i})$, ist $\sqrt{2} + \mathrm{i}$ ein primitives Elment für die Erweiterung $\mathbb{Q}(\sqrt{2}, \mathrm{i}) \mid \mathbb{Q}$.

Anwendungen

Der Satz vom primitiven Element ist für die Theorie sehr wichtig. Beispielsweise wird er für die Beweise folgender Sätze genutzt:

- Hauptsatz der Galoistheorie
- Zu jeder endlichen und separablen Erweiterung $E|K$ lässt sich ein Oberkörper $L \supseteq E \supseteq K$ finden, sodass $L|K$ normal ist. (Übungsaufgabe!)

Arturoverfahren zur Bestimmung eines primitiven Elements

Sei eine endliche und separable Körpererweiterung $L|K$ gegeben. Wenn man schon die Galoisgruppe G der Erweiterung kennt, kann man folgende Schritte durchführen, um ein primitives Element zu finden:

1. Zunächst rät man ein Element $z \in L$ von dem man hofft, dass $L = K(z)$ gelten könnte.

   Wenn $L = K(x, y)$, sollte man $z := x + y$ und dann $z := x + 2y$ versuchen.

2. Dann bestimmt man die Anzahl der Element der Menge

   $$H := \{\sigma(z) \mid \sigma \in G\}.$$

   Das ist nicht ganz einfach, weil man Teilergebnissen $\sigma_1(z), \sigma_2(z)$ nicht ansieht, ob sie gleich oder verschieden sind. Dazu schreibt man die Ergebnisse am besten in einer K-Basis von L aus, dann genügt es, Koeffizienten zu vergleichen.

3. Wenn $|H| = [L : K]$, ist z in der Tat ein primitives Element. Falls aber $|H| < [L : K]$, war die Vermutung leider falsch. Der Fall $|H| > [L : K]$ kann nicht eintreten.

Beispiel

Sei $L := \mathbb{Q}(\sqrt{2}, \mathrm{i})$ über $K := \mathbb{Q}$. Die zugehörige Galoisgruppe haben wir in einer Beispielrechnung zum Hauptsatz der Galoistheorie schonmal berechnet; wir halten uns an die Notation von dort.

1. Vermutung: $z := \sqrt{2} + \mathrm{i}$
2. $H := \{\sigma_1(z), \ldots, \sigma_4(z)\} = \{\sqrt{2} + \mathrm{i},\ \sqrt{2} - \mathrm{i},\ -\sqrt{2} + \mathrm{i},\ -\sqrt{2} - \mathrm{i}\}$

   Da $1, \sqrt{2}, \mathrm{i}, \sqrt{2}\,\mathrm{i}$ eine $\mathbb{Q}$-Basis von L ist, sind diese vier Elemente in der Tat verschieden.
3. Da $[L : K] = 4 = |H|$, ist also z in der Tat ein primitives Element.

Fragen und Antworten

Aus euren Mails, habe aber noch nicht alle Fragen hier abgetippt. Leider ziemlich unstrukturiert beantwortet, und wahrscheinlich sind noch sinnentstellende Schreibfehler enthalten.

Gruppentheorie

1. *Zu Normalteilern: Seien aH und bH Linksnebenklassen von $H \subset G$. Dann ist äquivalent: $b^{-1}a \in H \Leftrightarrow aH = bH$. Wieso gilt bei „$\Rightarrow$“ die Inklusion „$\subseteq$“?*

   Sei $g \in aH$ beliebig. Dann gibt es ein $h \in H$ mit $g = ah$ und es gilt die Rechnung
   $$g = ah = bb^{-1}ah = b(b^{-1}ah).$$
   Dabei liegt das eingeklammerte Element in H, denn $b^{-1}a$ liegt nach Voraussetzung in H, h sowieso, und H ist eine Untergruppe. Damit haben wir also g als ein Element von bH erkannt.

Lineare Algebra

1. *Warum schreibt man Basen als Tupel und nicht als Menge?*

   In der Tat schreiben manche Dozenten Basen auch als Mengen, aber die Tupelschreibweise ist die eigentlich richtige. Das mag zunächst verwirren, denn ob eine Liste von Vektoren eine Basis ist, hängt nicht von der Reihenfolge der Vektoren ab.

   Es macht in der linearen Algebra einen Unterschied: Da wird man lineare Abbildungen $f\colon V \to W$ als Matrizen darstellen, und zwar bezüglich beliebiger Basen in V und in W. Die resultierenden Matrizen hängen dann von der Reihenfolge der Basiselemente ab.

   Es gab ja auch die eine Übungsaufgabe, in der man die Darstellungsmatrix aufstellen sollte. Das war ein Spezialfall, nämlich für den Fall, dass man im Quell- und Zielraum jeweils die „kanonische Basis“ (e_1, e_2, e_3) (mit $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$) verwendet hat.

Ringtheorie

1. *Wie berechnet man die Inversen von Äquivalenzklassen $[g]$ in Faktorringen der Form $K[X]/(f)$?*

   Dazu kann man folgende Schritte durchführen:

   a) Den größten gemeinsamen Teiler d von f und g bestimmen.

b) Eine Bézoutdarstellung finden: $d = af + bg$ für gewisse $a, b \in K[X]$.

Am besten erledigt man diese beiden Schritte einfach in einem Aufwasch mit dem euklidischen Algorithmus (mit anschließendem Rückwärtsauflösen).

c) Ist d invertierbar (also ist d ein konstantes Polynom)? Dann ist die Äquivalenzklasse $[g]$ invertierbar und das Inverse ist $[d^{-1}b]$. Wenn d nicht invertierbar ist, ist auch $[g]$ nicht invertierbar.

2. *Wie berechnet man Inverse in Faktorringen der Form $\mathbb{Z}/(m)$?*

Wenn m klein ist, macht man das am besten durch Ausprobieren. Wenn m groß ist, kann man dieselben drei Schritte wie bei $K[X]/(f)$ verwenden.

3. *Kann ich sagen, dass wenn ein Produkt in einem Körper liegt, dass dann auch beide Faktoren im Körper liegen?*

Nein, Gegenbeispiel: $\pi \cdot \frac{1}{\pi}$ liegt in $\mathbb{Q}$, aber weder π noch $\frac{1}{\pi}$ liegen in $\mathbb{Q}$.

4. *Was bedeutet nochmal $\mathfrak{a} \lhd R$?*

Dass $\mathfrak{a}$ ein Ideal des Rings R ist.

5. *Wenn ich den Quotientenkörper $Q := \mathrm{Quot}(R)$ über einem faktoriellen Ring R betrachte, dann ist $Q[X]$ aber immer ein nullteilerfreier Hauptidealring oder?*

Ja, stimmt! Allgemeiner ist $K[X]$ für jeden Körper K (und nicht nur für irgendwelche Quotientenkörper) ein nullteilerfreier Hauptidealring (und auch ein euklidischer Ring).

Würde es auch reichen, wenn R nur nullteilerfrei ist, damit $Q[X]$ ein nullteilerfreier Hauptidealring ist?

Ja – wenn R nicht nur nullteilerfrei ist, sondern auch ein Integritätsbereich (die einzige Eigenschaft, die dazu noch fehlt, ist, dass $1 \neq 0$ in R). Denn wenn R kein Integritätsbereich ist, haben wir den Quotientenkörper Q gar nicht definiert. (Aus gutem Grund: Denn wenn $0 = 1$ sein sollte, können wir also gar nichts in die Nenner schreiben!)

(Begründung: Jeder euklidische Ring ist ein Hauptidealring, und für jeden Körper K ist der Polynomring $K[X]$ ein euklidischer Ring (da man die übliche Polynomdivision zur Verfügung hat).)

6. *Wenn ich dann den Polynomring in mehreren Variablen betrachte, dann gilt das mit dem Hauptidealring eigentlich nie oder?*

Genau! Das Ideal (X, Y) von $K[X, Y]$ ist stets ein Gegenbeispiel.

7. *Ist der Faktorring der Ring, der die Repräsentanten der Ideale im Ring „sammelt“?*

Fast! Also definiert ist der Faktorring R/I als die Menge aller Äquivalenzklassen von Elementen aus R bezüglich der Äquivalenzrelation

$$x \sim y \quad :\Leftrightarrow \quad x - y \in I.$$

Beispielsweise ist $\mathbb{Z}/(4)$ die Menge

$$\mathbb{Z}/(4) = \{[0], [1], [2], [3], [4], [5], [6], \ldots, [-1], [-2], [-3], \ldots\}.$$

Nun ist es aber so, dass in dieser Aufzählung von Äquivalenzklassen viele doppelt vorkommen: $[0] = [4]$ (da $0 \sim 4$), $[1] = [5]$ (da $1 \sim 5$), $[2] = [6]$ (da $2 \sim 6$) usw. Man kann also auch einfach schreiben:

$$\mathbb{Z}/(4) = \{[0], [1], [2], [3]\}.$$

Jetzt kann man nachrechnen, dass diese vier angegebenen Äquivalenzklassen wirklich paarweise verschieden sind (also 0 nicht äquivalent zu 1; 0 nicht äquivalent zu 2; 0 nicht äquivalent zu 3; 1 nicht äquivalent zu 2; 1 nicht äquivalent zu 3; 2 nicht äquivalent zu 3), weswegen man diese Darstellung nicht noch weiter vereinfachen kann.

Die Repräsentanten der Äquivalenzklassen, die in dieser letzten Darstellung noch vorkommen, bilden ein „vollständiges minimales Repräsentantensystem“. Wenn man jetzt noch mag, kann man die Äquivalenzklassenklammern auch weglassen und einfach $\mathbb{Z}/(4) = \{0, 1, 2, 3\}$ schreiben. Obwohl das relativ verbreitet ist, finde ich persönlich das aber weniger gut: Denn bei der Schreibweise mit den Äquivalenzklassenklammern wird man gleich daran erinnert, dass man es mit Äquivalenzklassen usw. zu tun hat.

8. *Bei den Idealen von Körpern: Kann man sagen, welche Elemente im Nullideal sind? Vermutlich die 0 und?*

   Nicht nur bei Körpern ist definiert: Das Nullideal ist stets die Teilmenge $\{0\}$, also diejenige Teilmenge des Rings, die genau ein Element enthält, und zwar das Nullelement.

   Das gilt sogar für den ominösen Nullring. Da in diesem $0 = 1$ gilt, also die Null des Rings dasselbe wie die Eins des Rings ist, könnte man da auch"$\{0\} = \{1\}$ schreiben.

9. *Zur Vorlesung: Bei $L|K$ Körpererweiterung, $a \in L$ ist ja $K(a)$ definiert. Dieses a ist aber speziell nicht aus K?*

   Genau, im Allgemeinen ist a aus L. Es kann aber auch mal aus K sein – das ist aber "langweilig", denn $K(a) = K$, wenn a in K liegt. (Wieso?)

10. *Was ist der Unterschied zwischen $K(v)(y) : K(v)]$ und $[K(y) : K(v)]$?*

    Also ersteres kann man ja einfach durch den Grad des Minimalpolynoms von y über $K(v)$ berechnen.

    Letzteres dagegen ist oftmals nicht definiert! Denn man $[L : K]$ kann nur dann schreiben, wenn K ein Unterkörper von L ist. Wenn jetzt y und v völlig beliebig sind, kann man daher nicht $[K(y) : K(v)]$ schreiben (wohl aber $[K(v)(y) : K(v)]$, denn nach einer der Rechenregeln für Körpererweiterungen gilt $K(v) \subseteq K(v, y) = K(v)(y)$).

    Sollte ausnahmsweise doch $K(v)$ eine Teilmenge von $K(y)$ sein, dann gilt wiederum $K(y) = K(v)(y)$ (wieder wegen der Rechenregeln), sodass es dann keinen Unterschied zwischen den beiden Ausdrücken gibt.

11. *Bei uns Lemma 10.2:* $\operatorname{inh}(fg) \sim \operatorname{inh}(f)\operatorname{inh}(g)$. *Ist die Schlange hier die Relation oder was soll hier überhaupt ausgesagt werden?*

    Mit „inh“ ist der sog. Inhalt eines Polynoms, mit der Schlangenrelation die Relation „ist assoziiert zu“ gemeint.

    Hier ein bisschen Kontext: Der Inhalt eines Polynoms mit ganzzahligen Koeffizienten ist definiert als der größte gemeinsame Teiler seiner Koeffizienten, also beispielsweise $\operatorname{inh}(5X^2 + 25X - 15X) = 5$.

    Diese Definition beinhaltet eine Schwierigkeit, denn im Allgemeinen ist der größte gemeinsame Teiler nicht eindeutig – im Beispiel hätte man genauso gut -5 statt $+5$ nehmen können.

    Es gilt also: Der ggT ist nicht eindeutig – aber zumindest sind je zwei ggT's „zueinander assoziiert“. Letzteres bedeutet, dass es ein invertierbares Element u des Rings gibt, sodass der eine ggT das Produkt von u mit dem anderen ggT ist. (Im Beispiel wäre $u = -1$.)

    Folglich ist auch der Inhalt nicht eindeutig definiert, sondern nur „bis auf Einheiten“ oder „bis auf Assoziiertheit“. Wenn man das verinnerlicht, ist es klar, dass die Gleichung $\operatorname{inh}(fg) = \operatorname{inh}(f)\operatorname{inh}(g)$ im Allgemeinen sicher nicht gelten kann – denn je nachdem, welche Wahlen der ggT's man für die drei Inhalte trifft, kommen auf den beiden Seiten der Gleichung verschiedene Ergebnisse 'raus.

    Es gilt allerdings „das nächstbeste“. Und zwar sind die Elemente $\operatorname{inh}(fg)$ und $\operatorname{inh}(f)\operatorname{inh}(g)$ im Allgemeinen zwar nicht gleich, aber zumindest zueinander assoziiert.

    Im Fall des Rings der ganzen Zahlen also wären $\operatorname{inh}(fg)$ und $\operatorname{inh}(f)\operatorname{inh}(g)$ stets vom Betrag her gleich.

12. *Was ist der Unterschied zwischen einem Polynom und einer Polynomfunktion?*

    Zu einem Polynom $f(X)$ mit Koeffizienten aus einem Ring R ist die Polynomfunktion ja als

    $$R \longrightarrow R, x \longmapsto f(x)$$

    definiert (großes „X“: die formale Polynomvariable, kleines „x“: ein beliebiges Element aus R).

    Auf den ersten Blick überraschend kann sein, dass manchmal die zugehörige Polynomfunktion null ist, obwohl das untersuchte Polynom nicht null ist. Das ist beispielsweise bei $f := X^2+X$ über dem Körper mit zwei Elementen $(\mathbb{Z}/(2))$ der Fall: Sowohl $f(0)$ als auch $f(1)$ sind null, aber f ist nicht das Nullpolynom.

    Es gibt übrigens einen Grund, wieso man in der Schule und in der Analysis nicht auf den Unterschied zwischen Polynom und Polynomfunktion achtet: Das im vorigen Absatz beschriebene Phänomen kann über Körpern, die unendlich viele Elemente enthalten, – und nur solche betrachtet man in der Schule und der Analysis – nämlich nicht auftreten (dass das so ist, ist nicht offensichtlich; wenn das interessiert, kann ich es gerne erklären).

13. *Wenn $\varphi\colon R \to S$ ein Ringisomorphismus ist. Ist es richtig, dass wenn zwei Ringe isomorph sind, dass sie dann tatsächlich im Grunde vollkommen gleich sind? Bedeutet dies dass man den Ringelementen in S nur die Namen der Ringelemente in R geben müsste um damit R zu erhalten? Also dass sich alle Ringelemente in R bzgl. der Verknüpfungen $\cdot$ und $+$ in R genauso verhalten wie ihre "Partnerünter anderem Namen in S bzgl. $\cdot$ und $+$ in S? Also dass die Verknüpfungen mit den jeweiligen Partnerelementen dasselbe tun?*

    Das ist alles absolut richtig! (Nur eine winzige Minimalanmerkung: Sie sind trotzdem nicht „gleich“ im mathematischen Sinn. Also es stimmt nicht, dass $R = S$ – eben weil die Namen der Ringelemente vielleicht verschieden sind.)

14. *Was ist dann noch der genaue Unterschied zum Automorphismus?*

    Automorphismen sind spezielle Arten von Isomorphismen $\varphi\colon R \to S$, nämlich solche, bei denen $R = S$ ist. Also ist jeder Automorphismus auch ein Isomorphismus, aber nicht umgekehrt.

    Den Begriff gibt es nur, um Schreibarbeit zu sparen: Statt „Isomorphismus von R nach R“ kann man einfach sagen „Automorphismus von R“.

15. *Häufig kommt vor, dass etwas "gleich ist bis auf Isomorphie". Was bedeutet das?*

    Also wenn zwei Ringe R uns S „gleich bis auf Isomorphie“ sind, meint einfach, dass die Ringe R und S zueinander isomorph sind.

    Die Satzkonstruktion „bis auf ...“ gibt es noch an anderen Stellen, zum Beispiel könnte man sagen „$4 = -4$ bis auf Vorzeichen“ oder (leicht scherzhaft) „$2 + 2 = 5$ bis auf Rechenfehler“.

16. *Es gibt auch irgendwie eine kanonische und eine nicht-kanonische Isomorphie.*

    Genau. Es gibt insgesamt vier relevante Adjektive: eindeutige, nicht-eindeutige, kanonische, nicht-kanonische Isomorphie.

    Zwei Ringe R und S heißen zueinander „eindeutig isomorph“, wenn es genau einen Isomorphismus von R nach S gibt. Ein Beispiel: Sei R der Ring $\mathbb{Z}/(2)$, also der Körper mit zwei Elementen, und sei S derselbe Ring, nur dass man auf jedes Element eine Schlange setzt. Dann gibt es genau einen Isomorphismus von R nach S (der muss nämlich die 0 von R auf die $\tilde{0}$ von S und die 1 von R auf die $\tilde{1}$ von S) schicken.

    Ein anderes Beispiel: Je zwei Körper mit p Elementen, wobei p eine feste Primzahl ist, sind zueinander eindeutig isomorph.

    Zwei Ringe R und S heißen zueinander „nicht-eindeutig isomorph“, wenn es mehr als einen Isomorphismus von R nach S gibt. Beispielsweise gibt es genau zwei Isomorphismen von $\mathbb{Q}(\sqrt{2})$ nach $\mathbb{Q}(\sqrt{2})$ (zum einen die Identitätsabbildung, zum anderen die Abbildung $a + b\sqrt{2} \mapsto a - b\sqrt{2}$).

    Je zwei Körper mit p^n Elementen, wobei p eine feste Primzahl und n eine natürliche Zahl ≥ 2 ist, sind zueinander isomorph, aber nicht eindeutig isomorph. (Das ist nicht offensichtlich.)

„Nicht-kanonisch“ ist das Gegenteil von „kanonisch“.

Schließlich ist „kanonisch“ nicht so leicht zu erklären: Das ist nämlich gar kein formaler mathematischer Begriff mit einer präzisen Definition, sondern eher ein umgangssprachlicher. Eine Abbildung heißt „kanonisch“, wenn man ihren Funktionsterm „ganz geradeaus“ und „ohne willkürliche Wahlen“ angeben kann.

Beispiele:

- Die Abbildung $R \to R, x \mapsto x$ findet man kanonisch.
- Dagegen würde man die Abbildung$\mathbb{Z} \to \mathbb{Z}, x \mapsto 17x$ nicht kanonisch finden (ein Ringhomomorphismus wäre sie übrigens auch nicht, aber das ist bei der Diskussion der Kanonizität nicht relevant): Hier kann sich der Leser die Frage stellen, wieso ausgerechnet 17, und nicht irgendeine andere Zahl, dransteht.
- Die Abbildung $R \to R/I, x \mapsto [x]$ findet man kanonisch.
- Die Abbildung $R \times S \to S \times R, (x, y) \mapsto (y, x)$ ebenso.
- Die Abbildung $\mathbb{R}^2 \to \mathbb{R}^2, (x, y) \mapsto (23x - 15y, x + 8y)$ ist nicht kanonisch.

Wenn man mehrere Abbildungben $R \to S$ betrachtet, ragen die kanonischen gewissermaßen besonders hervor. Statt „kanonisch“ sagt man manchmal auch „natürlich“. „Kanonisch“ und „eindeutig“ sind unabhängige Begriffe, es können also alle vier Kombinationen (nicht-)kanonisch/(nicht-)eindeutig auftreten.

Noch ein paar Alltagsbeispiele: Wenn mehrere Freunde ins Kino gehen und Sitzplätze in einer zusammenhängenden Reihe haben, gibt es natürlich keine eindeutige Sitzordnung, jeder kann sitzen, wo er mag. Es gibt aber manchmal (bis auf Spiegelung) eine kanonische Sitzordnung: Er, dann seine Freundin, dann ihre beste Freundin, dann deren Mutter.

Die Unterteilung des Jahres in Wochen zu je sieben Tagen ist nicht kanonisch: Prinzipiell hätte man eine Woche auch auf sechs oder acht Tage festsetzen können, die Wahl von sieben Tagen ist (wenn man die Situation nicht zu genau untersucht) willkürlich.

Dagegen ist der Begriff des Tages durchaus kanonisch: Denn der richtet sich ja nach der extern gegebenen Sonne.

17. *In der Vorlesung wurde gesagt, dass zum Beispiel zwei algebraische Abschlüsse eines Körpers K zueinander im Allgemeinen nicht-kanonisch isomorph sind wobei der Isomorphismus irgendwie die Identität erhält.*

    Mit dem Zusatz war wahrscheinlich gemeint, dass der Isomorphismus „Elemente aus K (er-/fest-)hält“. Und ja: Zwischen je zwei algebraischen Abschlüssen eines Körpers gibt es im Allgemeinen unendlich viele Isomorphismen, von denen keiner auf irgendeine Art und Weise spezieller/besonderer als die anderen wäre.

18. *Zum Quotientenkörper: Wie genau hat man sich die Äquivalenzklassen vorzustellen, also gibt es z. B. einen Zusammenhang zu Assoziiertheit? Oder dass*

man auf diese Weise schon vorhandene mögliche Inverse geschickt zusammenfasst.

Einen besonderen Zusammenhang zu Assoziiertheit sehe ich nicht. Eine Äquivalenzklasse $[(r, s)]$ von $\mathrm{Quot}(R)$ stellt man sich am Besten als Bruch $\frac{r}{s}$ vor. Dann sind die Definitionen der Addition und Multiplikation nämlich einfach die bekannten Bruchrechenregeln aus der Schule.

Vor allem bekommt man durch die Quotientenkörperkonstruktion jede Menge neuer Inverse! In $\mathrm{Quot}(R)$ ist in der Tat jedes Element $[(r, s)]$, was nicht gerade null ist, invertierbar: Das Inverse ist $[(s, r)]$. Das ergibt unter der Vorstellung als Brüche auch Sinn: Der Kehrbruch zu $\frac{r}{s}$ ist ja $\frac{s}{r}$.

19. *Es geht um $(d) = (a, b)$ in Hauptidealringen, wobei $d = \mathrm{ggT}(a, b)$. Wieso gilt diese Gleichheit?*

    Das liegt gar nicht so sehr an den Idealen, sondern vielmehr an der Definition des größten gemeinsamen Teilers! Hier ein Beweis der Aussage:

    Seien Elemente a, b in einem Hauptidealring R gegeben. Dann muss das Ideal (a, b) ein Hauptideal sein, also gibt es ein $d \in R$ mit $(a, b) = (d)$. Wir wollen jetzt zeigen, dass dieses d ein größter gemeinsamer Teiler von a und b ist. Dazu sind nach Definition des ggT's insgesamt zwei Dinge zu zeigen:

    – Es ist d ein Teiler von a und b. Denn da a ein Element von $(a, b) = (d)$ ist, ist a ein Vielfaches von d; und analog mit b.

    – Sei d' irgendein gemeinsamer Teiler von a und b. Dann müssen wir zeigen, dass d' ein Teiler von d ist. Da a und b Vielfache von d' sind, liegen a und b im Ideal (d'). Damit ist auch das ganze Ideal (a, b) eine Teilmenge von (d'). Also ist (d) eine Teilmenge von (d'), da $(d) = (a, b)$. Also ist d ein Vielfaches von d', oder anders gesagt ist d' ein Teiler von d.

    Nach demselben Muster kann man zeigen, dass $(a) \cap (b) = (\mathrm{kgV}(a, b))$ gilt.

Galoistheorie

1. *Ist es theoretisch immer möglich (also auch bei $[L : K] = \infty$) sukzessive algebraische Elemente dazu zu adjungieren und damit den algebraischen Abschluss zu erhalten. Also funktioniert diese Vorgehensweise theoretisch immer oder muss man bei unendlicher Dimension weitere Dinge beachten?*

    Ja, sie funktioniert immer – nur dass man dann vielleicht unendlich viele Elemente dazu adjungieren muss.

2. *Im Beweis zum Satz 11.2 wird $\alpha := X \bmod (g(X))$ gesetzt und es wird gesagt, dass $g(X)$ nun eine Nullstelle in L habe wobei L zunächst $K[X]/(g(X))$ (Kroneckerkonstruktion) ist und dann später umdefiniert wird. Wie hat man sich das vorzustellen bzw. wieso funktioniert das?*

    Eine tolle Frage! Ein bisschen Kontext: Die Behauptung ist ja, dass es zu jedem Polynom f mit Grad mindestens 1 über einem beliebigen Körper K

einen Zerfällungskörper gibt, also einen Oberkörper L von K, sodass f über L vollständig in Linearfaktoren $(X - x_1) \cdots (X - x_n)$ zerfällt und außerdem $L = K(x_1, ..., x_n)$ gilt, also jedes Element aus L sich als Summe, Differenz, Produkt, Quotient von Elementen aus K und den x_i's schreiben lässt.

Ein einfacher Fall wäre beispielsweise, dass das Polynom f konstant ist. Dann ist ja schon über K in Linearfaktoren zerfällbar (nämlich in sich selbst), womit K selbst ein Zerfällungskörper ist.

Ein anderer anschaulicher Fall ist der Fall $K = \mathbb{Q}$. Wenn man nämlich den Fundamentalsatz der Algebra glaubt, zerfällt f über $\mathbb{C}$ in Linearfaktoren; dann kann man für L einfach den entsprechenden Unterkörper von $\mathbb{C}$ nehmen.

Das besonders Interessante an dem Satz ist also, dass die Aussage auch für völlig beliebige (vielleicht „komische“) Körper stimmt, also auch für endliche Körper, sog. Funktionenkörper und viele weitere.

Der Beweis verläuft nun in zwei Schritten. Zunächst zeigt man, dass man über die Kroneckerkonstruktion $L := K[X]/(g)$ zunächst eine Erweiterung von K erhält, die zumindest eine Nullstelle von f enthält, nämlich $[X]$. Das ist gewissermaßen ein fauler Trick, die Nullstelle ist „künstlich“! Denn durch diese Konstruktion weiß man beispielsweise genauso wenig wie zuvor, was der genaue Zahlenwert der Nullstelle ist.

(Das ist ein bisschen so, wie in der Schule manchmal die komplexen Zahlen eingeführt werden: Man postuliert einfach, dass es eine neue Zahl „i“ gibt, die die Gleichung „$i^2 = -1$“ erfüllt; dann rechnet man damit. Einen Unterschied gibt es aber doch: Während man in der Schule die Existenz eines geeigneten „i“ nur postuliert hat, zeigen wir wirklich die Existenz des geeignetern Erweiterungskörpers L.)

Anschaulich kann man sich die künstliche Nullstelle nicht besonders gut vorstellen. Das liegt aber nicht nur an der Kroneckerkonstruktion, sondern auch einfach daran, dass man sich die Elemente eines beliebigen Körpers K nicht gut anschaulich vorstellen kann! Es gibt beispielsweise keine schöne Zahlengerade, auf der man die Körperelemente sinnvoll anordnen kann.

Zurück zum Beweis. Wir haben den Körper L definiert, der künstlich eine Nullstelle von f enthielt. Jetzt können zwei Fälle eintreten: Vielleicht haben wir Glück, und über dem Körper L zerfällt f schon in Linearfaktoren, dann können wir aufhören. Oder f zerfällt über L immer noch nicht vollständig in Linearfaktoren. Zumindest spaltet aber ein Linearfaktor ab, nämlich der, der zu der künstlichen Nullstelle gehört. Dann können wir dieselbe Konstruktion mit L statt K und dem restlichen Polynom statt f wiederholen. Auf diese Weise erhalten wir ein L'.

Dann können wieder zwei Fälle eintreten: Entweder, f zerfällt über L' in Linearfaktoren, oder wir müssen abermals die Kroneckerkonstruktion bemühen und ein L'' erhalten. Da aber bei jedem Konstruktionsschritt f mindestens eine weitere (künstliche) Nullstelle erhält, können wir nach spätestens $\deg f$ vielen Schritten aufhören.

Hier zwei Beispiele:

- Wir wollen den Beweis für den Fall $K = \mathbb{Q}$, $f = X^2 - 2$ nachvollziehen. Dann setzen wir $L := K[Y]/(Y^2 - 2)$. (Ich schreibe „Y“ statt „X“, um nicht mit der Polynomvariablen durcheinander zu kommen.) Dann gilt in L die Rechnung

  $$[Y]^2 - [2] = [Y^2 - 2] = [0] = 0,$$

  also besitzt das Polynom $X^2 - 2$ in L die künstliche Nullstelle $[Y]$. Außerdem gilt in $L[X]$

  $$(X - [Y])(X + [Y]) = X^2 - [Y^2] = X^2 - [2],$$

  also zerfällt f über L sogar schon völlig in Linearfaktoren, obwohl wir nur eine einzige künstliche Nullstelle adjungiert haben.

- Sei $K = \mathbb{Q}$, $f = X^3 - 2$. Dann setzen wir zuerst $L := K[Y]/(Y^3 - 2)$. Dann besitzt f die Nullstelle $[Y]$ in L. Wenn wir f durch $(X - [Y])$ polynomdividieren, erhalten wir

  $$f = (X - [Y])(X^2 + [Y]X + [Y]^2).$$

  Dabei ist der hintere Faktor leider irreduzibel (das ist nicht offensichtlich), also sind wir noch nicht fertig. Wir müssen also erneut die Kroneckerkonstruktion verwenden und definieren

  $$L' := L[Z]/(Z^2 + [Y]Z + [Y]^2).$$

  („Z“ statt „X“ oder „Y“, um Verwirrungen zu vermeiden.) Dann kann man nachrechnen, dass in $L'[X]$ die Rechnung

  $$f = (X - [[Y]])(X - [Z])(X + [[Y] + Z])$$

  gilt. Damit ist also L' der gesuchte Zerfällungskörper.

Eine gute Übung, um die Kroneckerkonstruktion zu üben, ist, die ausgelassenen Polynomdivisionen zu versuchen.

3. *In der Vorlesung wurde sehr oft betont, dass die Konstruktion mit $K[X]/(m_\alpha)$, wobei (m_α) das vom Minimalpolynom von α erzeugte Ideal ist, unabhängig von α ist und nur noch vom Minimalpolynom abhängt. Worin liegt genau der Vorteil und warum ist dies so wichtig für später?*

   Zunächst ist es schlichtweg interessant: Die Konstruktion scheint von α abzuhängen, weil ja α zur Konstruktion benötigt wird, stellt sich aber im Nachhinein als von α unabhängig heraus.

   Ein anderer Grund: Ohne die Erkenntnis mit der Kroneckerkonstruktion könnte man denken, dass der Körper $\mathbb{Q}(\sqrt[3]{2})$ ein sehr kompliziertes Objekt ist: Man benötigt scheinbar genaue Kenntnis der dritten Wurzel aus 2. Wie soll man diese berechnen? Welche Genauigkeit genügt? Wo liegt $\sqrt[3]{2}$ auf dem Zahlenstrahl? Usw.

Dann erkennt man, dass $\mathbb{Q}(\sqrt[3]{2})$ isomorph zu $\mathbb{Q}[X]/(X^3-2)$ ist. Dazu muss man bis auf die Definition der dritten Wurzel und einem allgemeinen Irreduzibilitätskriterium nichts genaues über $\sqrt[3]{2}$ wissen. Wenn man also nur an ring- bzw. körpertheoretischen Fragen interessiert ist, sind die Nachkommastellen von $\sqrt[3]{2}$ völlig unerheblich.

Daraus ergibt sich eine weitere erstaunliche Tatsache: Das Polynom X^3-2 hat ja (in $\mathbb{C}$) noch zwei weitere Nullstellen. Aus Sicht der Analysis sind die von der reellen dritten Wurzel aus 2 völlig verschieden. Aus Sicht der Ring- bzw. Körpertheorie sind sie aber (in einem gewissen Sinn) gar nicht zu unterscheiden!

(Übrigens: Früher fand man ja die komplexen Zahlen sehr mysteriös und es gab kontroverse Diskussionen darüber, ob sie tatsächlich existieren. Wenn man algebraisch an die Sache herangeht, ist es aber völlig klar: Man kann $\mathbb{C}$ als $\mathbb{R}[X]/(X^2+1)$ definieren. Für letzteres Objekt benötigt man nur die reellen Zahlen, Polynome und eine Äquivalenzrelation, also unstrittige Begriffe.)

4. *Stimmt es, dass die ganze Galoistheorie ausschließlich im Fall einer endlichen Körpererweiterung funktioniert und man damit im Fall einer unendlichen Körpererweiterung keinerlei Aussagen treffen kann?*

   Ja! Allerdings gibt es auch sog. unendliche Galoistheorie. :-) Eine große offene Frage ist beispielsweise, wie genau die Gruppe $\mathrm{Aut}_{\mathbb{Q}}(\bar{\mathbb{Q}})$, also die Gruppe der $\mathbb{Q}$-Automorphismen eines algebraischen Abschlusses von $\mathbb{Q}$, aussieht.