Vorlesung Lineare Algebra I

SoSe '24 hhu
K. Halupczok

§2: Algebraische Grundbegriffe

L8: Konkrete Gruppen, Ringe, Körper

Stichworte: Konstruktion der Zahlbereiche $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ mit Äquivalenzrelationen, komplexe Zahlen $\mathbb{C}$, Polynome, Polynomdivision, Nullstellenabspaltung

---

Konstruktion der Zahlbereiche

8.1. Äquivalenzrelationen werden sehr vielfältig eingesetzt, um neue mathematische Strukturen zu definieren (z.B. Quotientenvektorräume, Quotientenkörper, Randverklebungen...). Eine Hauptanwendung ist die Konstruktion der **Zahlbereiche**

$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, die wir hier angeben (natürlich gibt es viele andere Möglichkeiten, dies zu tun). Wir gehen dabei davon aus, dass die nat. Zahlen $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ bereits (axiomatisch) erklärt sind (was wir nicht näher vertiefen wollen; dahinter steckt u.a. das Prinzip der vollständigen Induktion). Ebenso sei bekannt, dass mit $(\mathbb{N}_0, +)$ und $(\mathbb{N}, \cdot)$ jeweils eine Halbgruppe mit Eins, nämlich 0 bzw. 1, gegeben ist.

8.2. **Def.:** $\mathbb{Z} := \mathbb{N}_0 \times \mathbb{N}_0 / \sim$ mit der Äquivalenzrelation

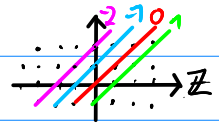
$(n, m) \sim (\mu, \nu) :\Leftrightarrow n + \nu = m + \mu$. ("$n - m$ = Konstante"...)

Darin ist $\mathbb{N}_0$ "eingebettet" in der Form $\{[(n, 0)] \mid n \in \mathbb{N}_0\}$.

Weiter: $[(n, m)] + [(\mu, \nu)] := [(n + \mu, m + \nu)]$.

Die Zahl $-n$ für $n \in \mathbb{N}_0$ liegt vor als $[(0, n)]$,

denn $[(n, 0)] + [(0, n)] = [(n, n)] = [(0, 0)]$.



beide Konstruktion spielt nur der 1. Quadrant $\mathbb{N}_0 \times \mathbb{N}_0$ eine Rolle!

Ü Wie geht die Definition von "$\cdot$" und "$\leq$"? (nicht naheliegend!)

Welche Eigenschaften haben $+, \cdot$ und $\leq$?

(Vgl. auch mit der Konstruktion in 8.3, die ähnlich ist.)

8.3. **Def.:** $\mathbb{Q} := \mathbb{Z} \times \underbrace{\mathbb{N}}_{\text{ohne } 0} / \sim$ mit der Äquivalenz-Relation

$$(z,n) \sim (y,m) :\Leftrightarrow zm = ny$$

Darin ist $\mathbb{Z}$ "eingebettet" in der Form $\{[(z,1)] \mid z \in \mathbb{Z}\}$.
Wir schreiben dann $\frac{z}{n}$ für $[(z,n)]$ und erhalten die üblichen Rechengesetze für $+, \cdot$, wenn wir erklären:

$$\frac{z}{n} \cdot \frac{y}{m} := \frac{zy}{nm}, \qquad \frac{z}{n} + \frac{y}{m} := \frac{zm+yn}{nm}.$$

Def. $\leq$: $\frac{z}{n} \leq \frac{y}{m} :\Leftrightarrow zm \leq yn$.

8.4. **Def.:** $\mathbb{R} := \mathcal{C}/\sim$ mit der Menge

$$\mathcal{C} := \{(a_n)_{n\in\mathbb{N}} \subseteq \mathbb{Q} \mid (a_n) \text{ ist Cauchyfolge in } \mathbb{Q}\}$$

$\forall \varepsilon > 0 \; \exists N_\varepsilon \; \forall n,m \geq N_\varepsilon : |a_n - a_m| < \varepsilon$

und der Äquivalenz-Relation $(a_n)_{n\in\mathbb{N}} \sim (b_n)_{n\in\mathbb{N}} :\Leftrightarrow (a_n - b_n)_{n\in\mathbb{N}}$ ist Nullfolge.

$\Leftrightarrow \forall \varepsilon > 0 \; \exists N_\varepsilon \; \forall n \geq N_\varepsilon : |a_n - b_n| < \varepsilon$

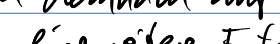
8.5. **Satz:** Der Körper der reellen Zahlen ist "der" (bis auf Isomorphie, vgl. 8.13) eindeutig bestimmte vollständige angeordnete Körper, der $\mathbb{Q}$ fortsetzt. (ohne Bew.)

8.6. **Def.:** Ein Körper K (mit Verknüpfungen $+, \cdot$) und einer strikten Anordnung "$<$" (die trichotomisch, d.h. $\forall x,y \in K: x<y \;\dot\vee\; x=y \;\dot\vee\; y<x$ mit "$\dot\vee$" für entweder - oder, und transitiv (17) ist) heißt angeordneter Körper,

falls $\forall x,y,z \in K: x<y \Rightarrow x+z < y+z$ (Monotonie der Addition)

und $\forall x,y,z \in K: x<y, z>0 \Rightarrow xz < yz$ (Monotonie der Multiplikation) gilt.

Mit einer strikten Anordnung $<$ def. man eine Anordnung "$\leq$" durch $x \leq y :\Leftrightarrow x<y \vee x=y$

8.7. Auf diesem Wege erreichen wir eine Fortsetzung der Zahlbereiche: $\mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.
S.1 haben alle die Eigenschaft, dass sie eine Anordnung "$<$" besitzen. Deren El. lassen sich demnach auf einem Zahlenstrahl anordnen: $\mathbb{R}$: 
Es gibt noch eine weitere Fortsetzung, man kann $\mathbb{R}$ zu einem Körper $\mathbb{C}$ fortsetzen:

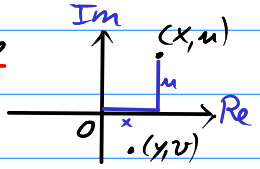
8.8. **Def.:** In $\mathbb{R}^2 = \{(x,u) \mid x,u \in \mathbb{R}\}$ def. $(x,u) + (y,v) := (x+y, u+v)$

und $(x,u) \cdot (y,v) := (xy - uv, xv + uy)$ für $x,y,u,v \in \mathbb{R}$.

8.9. **Satz:** Die Menge $\mathbb{R}^2$ ist mit diesen Verknüpfungen $+, \cdot$ ein Körper, der $\mathbb{R}$ und die Verknüpfungen $+, \cdot$ von $\mathbb{R}$ fortsetzt, vgl. 8.12.

8.10. **Def.:** Man nennt $(\mathbb{R}^2, +, \cdot)$ den **Körper der komplexen Zahlen.**
Dieser wird mit $\mathbb{C}$ bezeichnet.
Eine komplexe Zahl $z=(x,u) \in \mathbb{C}$ hat immer zwei reelle Komponenten, hier $x,u \in \mathbb{R}$.
Die 1. Komponente x von z heißt **Realteil**, $x = \operatorname{Re} z$,
die 2. Komponente der **Imaginärteil** $u = \operatorname{Im} z$.

komplexe Ebene $\mathbb{C}$:



8.11. **Bew. von Satz 8.9:** • Die Multiplikation ist offensichtlich kommutativ.
• Sie ist auch assoziativ:

$$\begin{aligned}((x,u)\cdot(y,v))\cdot(r,s) &= (xy-uv,\ xv+uy)\cdot(r,s)\\ &= \big((xy-uv)r-(xv+uy)s,\ (xy-uv)s+(xv+uy)r\big)\\ &= \big(x(yr-vs)-u(ys+vr),\ x(ys+vr)+u(yr-vs)\big)\\ &= (x,u)\cdot(yr-vs,\ ys+vr) = (x,u)\cdot\big((y,v)\cdot(r,s)\big)\end{aligned}$$

• Es gelten die Distributivgesetze; wegen der Kommutativität genügt es, eines davon nachzurechnen: (ü) • Die Multiplikation ist eine Verknüpfung auf $\mathbb{R}^2\setminus\{0,0\}$:
Seien $(x,u)\neq(0,0)\neq(y,v)$. Wäre $(x,u)\cdot(y,v)=0$, folgte $xy-uv=0$, $xv+uy=0$ und somit $0=(xy-uv)^2+(xv+uy)^2=(x^2+u^2)\cdot(y^2+v^2)$, also wäre $x^2+u^2=0$ $(\Leftrightarrow (x,u)=0)$ $\vee$ $y^2+v^2=0$ $(\Leftrightarrow (y,v)=0)$ ↯
• Das neutrale El. bzgl. $\cdot$ ist $(1,0)$, da $(x,u)\cdot(1,0)=(x,u)$.
• Das inverse El. zu $(x,u)\neq(0,0)$ ist $\left(\frac{x}{x^2+u^2}, \frac{-u}{x^2+u^2}\right)$. □

8.12. **Bem.:** Die Teilmenge $\mathbb{R}\times\{0\} = \{(x,0);\ x\in\mathbb{R}\}$ von $\mathbb{C}$ ist bzgl. der in $\mathbb{C}$ erklärten Addition und Multiplikation selbst ein Körper, und die Abbildung $f:\mathbb{R}\to\mathbb{R}\times\{0\}$, $x\mapsto(x,0)$ ist bijektiv und respektiert die Verknüpfungen $+,\cdot$, d.h. $f(x+y)=f(x)+f(y)$, $f(x\cdot y)=f(x)\cdot f(y)$ gilt für alle $x,y\in\mathbb{R}$. (⊛)
($+$ in $\mathbb{R}$, $+$ in $\mathbb{R}\times\{0\}$, $\cdot$ in $\mathbb{R}$, $\cdot$ in $\mathbb{R}\times\{0\}$)

"strukturgleich" Wir identifizieren $\mathbb{R}\times\{0\}$ daher mit $\mathbb{R}$ und sagen, die Teilmenge $\mathbb{R}\times\{0\}$ ist **isomorph** zu $\mathbb{R}$. Analog ist $\{0\}\times\mathbb{R}$ isomorph zu $\mathbb{R}$.

8.13. **Def.:** Zwei Körper K_1 und K_2 heißen **isomorph**, falls es eine bijektive Abb. $f: K_1\to K_2$ gibt mit (⊛) für alle $x,y\in K_1$. In diesem Fall heißt f ein **Körperisomorphismus.**

8.14. **Bem.:** Jede komplexe Zahl $z=(x,m)$ lässt sich darstellen als $z=(x,m)=(x,0)+(0,m)=(x,0)+(0,1)\cdot(m,0)$. Mit der Abkürzung $i:=(0,1)$ erhalten wir also $\underline{\underline{z = x + im}}$. (Man nennt i imaginäre Einheit.) Offenbar gilt $i^2=-1$. Statt $0+im$ schreibe im, statt $x+i\cdot 0$ schreibe x.

8.15. **Bem.:** Ist $z\in\mathbb{C}$, $z\neq 0$, schreiben wir für z^{-1} auch $\frac{1}{z}=\frac{1}{a+ib}$.
Ist z.B. $z=x+im$, $w=y+iv$, dann ist
$z\cdot w=(x+im)\cdot(y+iv)=xy+ixv+imy+i^2mv=(xy-mv,xv+my)$.
Ist $z\neq 0$, gilt $\frac{1}{z}=\frac{1}{x+im}=\frac{x-im}{(x+im)(x-im)}=\frac{x}{x^2+m^2}-i\frac{m}{x^2+m^2}$.
Mit $z=x+im\in\mathbb{C}$ ist auch $\bar{z}=x-im\in\mathbb{C}$. Die komplexe Zahl $\bar{z}$ heißt die zu z konjugiert komplexe Zahl.

8.16. **Satz:** Es gilt für alle $z,w\in\mathbb{C}$: (i) $\overline{z+w}=\bar{z}+\bar{w}$, $\overline{z\cdot w}=\bar{z}\cdot\bar{w}$,
(ii) $\overline{(\bar{z})}=z$, (iii) $z\in\mathbb{R}\Leftrightarrow z=\bar{z}$, (iv) $z\cdot\bar{z}\geq 0$ und $z\cdot\bar{z}=0\Leftrightarrow z=0$.

8.17. **Def.:** Die reelle Zahl $(z\cdot\bar{z})^{1/2}$ heißt der Betrag von z. **Bew.:** (ii)

8.18. **Satz:** $\mathbb{C}$ ist nicht anordenbar, d.h. nicht so, dass die Multiplikation monoton ist.
Bew.: Klar: $i\neq 0$. Wäre "$<$" eine Anordnung und $i>0$, folgte $i\cdot i>i\cdot 0$, d.h. $-1>0$ ↯.
Wäre $i<0$, folgte $-i>0$, also $(-i)\cdot(-i)>(-i)\cdot 0$, also wieder $-1>0$ ↯. □

[Beachte: $-1>0$ ist ein ↯, denn daraus folgt (mal (-1)): $1>0$, mit $-1>0$ folgt $0>0$ ↯ zur Trichotomie.]

Polynome: Gegeben sei ein Körper K.

8.19. **Def.:** Ein Polynom P über K ist eine Folge $a_0,a_1,a_2,\ldots,a_n,a_{n+1},\ldots$ von Körperelementen, deren El. ab einer Stelle alle $=0$ sind, d.h. $\exists n\in\mathbb{N}\ \forall k>n$: $a_k=0$. Also: $P=(a_0,a_1,\ldots,a_n,0,0,\ldots)$. Wir schreiben in symbolischer Form $P=a_0+a_1X+a_2X^2+\ldots+a_nX^n$ oder auch $P=\sum_{i=0}^{n}a_iX^i$, oder auch $P=a_nX^n+a_{n-1}X^{n-1}+\ldots+a_1X+a_0$. Ein Polynom der Form X^i heißt ein Monom. Das Polynom $P=(0,\ldots,0)$ heißt Nullpolynom, Kurz: $P=0$.
Ist $P\neq 0$, heißt $n=\max\{k\in\mathbb{N}_0;\ a_k\neq 0\}$ der Grad von P und a_n heißt dann der Leitkoeffizient von P. Schreiben: $\deg P=n$, es sei $\deg 0:=-1$ (auch: $-\infty$).
Ist der Leitkoeffizient $=1$, so heißt das Polynom normiert.
Die Menge aller Polynome über K bezeichnen wir mit $K[X]$. Man nennt X die Unbestimmte eines Polynoms. Polynome vom Grad 1 heißen linear.

8.20. **Bsp.:** $P=X^2+2X-3\in\mathbb{R}[X]$ hat $\deg P=2$, $Q=X^4-iX\in\mathbb{C}[X]$ hat $\deg Q=4$.

8.21. Wir führen auf $K[X]$ eine Addition und Multiplikation ein, so dass formal wie mit Körperelementen gerechnet werden kann, wie z.B. $(a_0 + a_1 X) \cdot (b_0 + b_1 X + b_2 X^2) = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + (a_0 b_2 + a_1 b_1) X^2 + a_1 b_2 X^3$.

8.22. **Def.**: Für Polynome $P = a_0 + a_1 X + \ldots + a_n X^n$ und $Q = b_0 + b_1 X + \ldots + b_m X^m$ in $K[X]$ mit $n \geq m$, man setze dabei $b_{m+1} := 0, \ldots, b_{n-1} := 0, b_n := 0$ falls $m < n$, def. $P + Q := (a_0 + b_0) + (a_1 + b_1) X + \ldots + (a_n + b_n) X^n \in K[X]$. und $P \cdot Q := c_0 + c_1 X + \ldots + c_{n+m} X^{n+m} \in K[X]$ mit $c_i = \sum_{k=0}^{i} a_k b_{i-k}$, d.h. $c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, ... usw.

8.23. **Satz**: $(K[X], +, \cdot)$ ist kommutativer Ring mit 1 (genannt Polynomring).

Bew.: Da die Verknüpfung $+$ praktisch in K^n mit geeignetem n ausgeführt wird, ist unmittelbar klar, dass $(K[X], +)$ eine abelsche Gruppe ist; das neutr. El. ist das Nullpolynom 0, und inverses El. zu $P = a_0 + a_1 X + \ldots + a_n X^n$ ist $-P := (-a_0) + (-a_1) X + \ldots + (-a_n) X^n$. Die Assoziativität von $\cdot$ und die Distributivgesetze ergeben sich durch Nachrechnen (ü). wegen $\sum_{l=0}^{i} a_l b_{i-l} \overset{i-l=:k}{=} \sum_{k=0}^{i} a_{i-k} b_k = \sum_{k=0}^{i} b_k a_{i-k}$ ist $P \cdot Q = Q \cdot P$, die Multiplikation also kommutativ. Das konstante Polynom $1 = 1 + 0 \cdot X + 0 \cdot X^2 + \ldots$ ist das Einselement. □

8.24. **Bem.**:
- Für alle Polynome $P, Q \in K[X]$ gilt: $\deg(P+Q) \leq \max(\deg P, \deg Q)$, und ist $P \neq 0 \neq Q$, gilt: $\deg(P \cdot Q) = \deg(P) + \deg(Q)$,
- Jedes Polynom $P = a_0 + a_1 X + \ldots + a_n X^n$ erzeugt eine Fkt. auf K, die **Polynomfunktion** $K \to K$, $x \mapsto a_0 + a_1 x + \ldots + a_n x^n$.

8.25. **Satz (Polynomdivision)**: Zu Polynomen $P, Q \in K[X]$, $Q \neq 0$, ex. eindeutig bestimmte Polynome $R, S \in K[X]$ mit $P = S \cdot Q + R$ und $\deg R < \deg Q$.

8.26. **Bem.**: Man nennt dann R den **Rest** der **Polynomdivision von P durch Q**, und S den **Quotienten** (der ...''...). Polynomringe erlauben also eine Division mit Rest, genau wie im Ring $\mathbb{Z}$ (wie etwa $253 : 17 = 14$, $\frac{17}{83}$, $\frac{68}{15}$ ← Rest 15. Also: $253 = 14 \cdot 17 + 15$, $P = S \cdot Q + R$).

8.27. **Beweis von Satz 8.25:**

• Existenz von R und S: Klar für $\deg P < \deg Q$: dann ist $S = 0$, $R = P$.

o.E. o.B.d.A. Somit können wir o.E. $\deg P \geq \deg Q$ annehmen.

Dann führen wir eine vollst. Ind. nach $n = \deg P$:

Ind.anf.: $n = 0$: Dann ist $P = a_0$, $a_0 \neq 0$, und auch $\deg Q = 0$, also $Q = b_0 \neq 0$.
Haben dann $P = a_0 b_0^{-1} Q + 0$.

Ind.schritt: $\deg P \leq n-1 \rightsquigarrow \deg P = n$: Seien $P = a_0 + a_1 X + \ldots + a_n X^n$, $a_n \neq 0$,
und $Q = b_0 + b_1 X + \ldots + b_m X^m$, $b_m \neq 0$,
und $m \leq n$. Betr. $P_1 := P - \frac{a_n}{b_m} X^{n-m} \cdot Q$ mit $\deg P_1 < n$. "Echt kleiner n"
Für $\deg P_1 < \deg Q$ folgt nach obigem, für $\deg P_1 \geq \deg Q$ folgt nach Induktionsvor., dass $\exists R_1, S_1 \in K[X]: P_1 = S_1 Q + R_1$, $\deg R_1 < \deg Q$.
Dann folgt $P = \left(S_1 + \frac{a_n}{b_m} X^{n-m}\right) \cdot Q + R_1$ mit $\deg R_1 < \deg Q$.
Also: $S = S_1 + \frac{a_n}{b_m} \cdot X^{n-m}$, $R = R_1$ liefert die Ind.beh.

• Eindeutigkeit: Aus $P = S_1 Q + R_1$, $\deg R_1 < \deg Q$ und $P = S_2 Q + R_2$, $\deg R_2 < \deg Q$,
folgt durch Differenzenbildung: $R_2 - R_1 = (S_1 - S_2) \cdot Q$. Wäre $S_1 - S_2 \neq 0$, folgte
mit $\deg Q \leq \deg(R_2 - R_1) \leq \max(\deg R_2, \deg R_1)$ ein Widerspruch.
Also gild doch $S_1 = S_2$ und damit auch $R_1 = R_2$. □

8.28. **Bsp.:** • Sei $P = X^4 - 5X^3 + 3X^2 - 10X + 2$ und $Q = X^2 - 5X + 1$.

Division mit Rest:

$$(X^4 - 5X^3 + 3X^2 - 10X + 2) : (X^2 - 5X + 1) = X^2 + 2$$

$\rightsquigarrow X^2 \cdot Q$: $\quad -(X^4 - 5X^3 + X^2)$

$$2X^2 - 10X + 2 \quad \leftarrow \text{soviele Summanden vernachlässigen, bis es soviele wie in } 2 \cdot Q \text{ sind}$$

$\rightsquigarrow 2 \cdot Q$: $\quad -(2X^2 - 10X + 2)$

$$0 \quad \leftarrow \text{Rest, Rechnung geht auf.}$$

Also: $P = Q \cdot (X^2 + 2)$.

• Sei $P = X^3 + 1$, $Q = X - 1$. Dann: $(X^3 + 1) : (X - 1) = X^2 + X + 1 + \frac{2}{X-1}$

$X^2 \cdot Q$: $\quad -(X^3 - X^2)$

$$X^2 + 1$$

$X \cdot Q$: $\quad -(X^2 - X)$

$$X + 1$$

$1 \cdot Q$: $\quad -(X - 1)$

$$2 \quad \leftarrow \text{Rest} \neq 0, \text{ Rechnung geht nicht auf}$$

Also: $P = Q \cdot (X^2 + X + 1) + 2$.

Nullstellenabspaltung

8.29. **Def.:** Ein El. $x_0 \in K$ heißt **Nullstelle des Polynoms** $P \in K[X]$, wenn x_0 Nullstelle der zugeh. Polynomfkt. $K \to K$, $x \mapsto P(x)$ ist, also $P(x_0) = 0$ gilt.

8.30. **Kor.:** Genau dann ist x_0 Nullstelle eines Polynoms $P \in K[X]$, wenn es eine Faktorisierung $P = (X - x_0) \cdot S$ mit $S \in K[X]$ gibt.
d.h. Zerlegung in ein Produkt (von nichttrivialen Faktoren) "Nullstellenabspaltung"

Bew.: Ist x_0 Nullstelle von P, so erhalten wir als Spezialfall von Satz 8.25 für P die Darstellung $P = S \cdot (X - x_0)$ mit $S \in K[X]$. Umgekehrt folgt aus dieser Darstellung unmittelbar, dass x_0 Nullstelle von P ist. □

8.31. **Bem.:**
- Ein Polynom vom Grad $n \geq 0$ hat höchstens n p.w.v. Nullstellen. (paarweise verschiedene)
- Ein Faktor der Form $X - x_0$ heißt Linearfaktor.
- Ist K unendlich, so gehören zu $P, Q \in K[X]$, $P \neq Q$, auch verschiedene Polynomfunktionen. Wäre nämlich $P(X) = Q(X)$ für alle $x \in K$, so hätte $P - Q$ unendl. viele Nullstellen.
- Nicht jedes Polynom besitzt eine Nullstelle, wie z.B. $X^2 + 1 \in \mathbb{R}[X]$. Als Polynom in $\mathbb{C}[X]$ aufgefasst hat es aber Nullstellen, nämlich $i, -i$. Dies gilt für jedes Polynom in $\mathbb{C}[X]$ aus 8.32:

8.32. **Fundamentalsatz der Algebra:** Jedes Polynom $P \in \mathbb{C}[X]$ vom Grad $\deg P \geq 1$ besitzt eine Nullstelle (in $\mathbb{C}$). [ohne Beweis, z.B. Funktionentheorie, Analysis]

Daraus folgt sofort:

8.33 **Kor.:** Jedes Polynom P über $\mathbb{C}$ mit $\deg P \geq 1$ zerfällt vollständig in Linearfaktoren, d.h. ist Produkt von Polynomen vom Grad 1.

8.34 **Bsp.:**
- $X^4 - 5X^3 + 3X^2 - 10X + 2 = (X^2 - 5X + 1) \cdot (X^2 + 2)$
$= \left(X - \frac{5}{2} - \frac{\sqrt{21}}{2}\right) \cdot \left(X - \frac{5}{2} + \frac{\sqrt{21}}{2}\right) \cdot (X - i\sqrt{2}) \cdot (X + i\sqrt{2})$
- $X^3 - 2X^2 + X = X \cdot (X^2 - 2X + 1) = X \cdot (X - 1)^2$

8.35 Es ist möglich, $\mathbb{C}$ auch auf andere Weise zu konstruieren, beispielsweise so:
Sei $\mathbb{C} := \mathbb{R}[X]/\sim$ mit den reellen Polynomen $\mathbb{R}[X] = \{\sum_{i=0}^{n} a_i X^i;\ n \in \mathbb{N}_0, a_i \in \mathbb{R}\}$
und der $\sim$-Relation $f(X) \sim g(X) :\Leftrightarrow \exists\, h(X) \in \mathbb{R}[X]$:

$$f(X) - g(X) = h(X) \cdot (X^2 + 1).$$

$\rightarrow$ die $\sim$-Klassen sind El. von $\mathbb{C}$ und wir erklären $+, \cdot$ durch

$$\circledast \begin{cases} [f(X)] + [g(X)] := [f(X) + g(X)] \\ [f(X)] \cdot [g(X)] := [f(X) \cdot g(X)] \end{cases}$$

← deutlich natürlichere Def. als in 8.8!

Jede Klasse $[f(X)]$ enthält genau ein Polynom der Form $a_0 + a_1 X$
ist also durch ein Zahlenpaar (a_0, a_1) eindeutig bestimmt, die wieder
auf Real- und Imaginärteil führen.

Beachten Sie:

$[X^2 + 1] = [0]$, und weiter ist

$$[X] \cdot [X] = [X^2] = [X^2 + 1 - 1] = [X^2 + 1] + [-1] = [-1],$$

d.h. $[X]$ ist eine Zahl mit $[X]^2 = [-1]$,
die würden wir ja wohl "i" nennen...

Mit der Abbildung $\mathbb{R}^2 \to \mathbb{R}[X]/\sim$
$(x, u) \mapsto [x + u \cdot X]$ erhalten wir einen
Körperisomorphismus, also "nichts Neues."

d.h. $\mathbb{C}$ als $(\mathbb{R}^2, +, \cdot)$ wie in 8.8.–8.10. konstruiert