D-MATH Algebra I HS 2022
Prof. Richard Pink

Musterlösung Wiederholungsserie

1. Beweise für beliebige Untergruppen $H_1 < G > H_2 > H_2'$ die Ungleichungen

   (a) $[H_1 : H_1 \cap H_2] \leqslant [G : H_2]$.

   (b) $[G : H_1 \cap H_2] \leqslant [G : H_1] \cdot [G : H_2]$.

   (c) $[H_1 \cap H_2 : H_1 \cap H_2'] \leqslant [H_2 : H_2']$.

   Lösung: (a) Betrachte die Linksoperation von H_1 auf G/H_2 durch Linkstranslation $(h_1, gH_2) \mapsto h_1 g H_2$. Der Stabilisator der trivialen Nebenklasse H_2 ist die Menge aller $h_1 \in H_1$ mit $h_1 H_2 = H_2$, was äquivalent ist zu $h_1 \in H_2$; der Stabilisator ist also $H_1 \cap H_2$. Die Bahn des Elements $H_2 \in G/H_2$ unter H_1 hat folglich die Länge $[H_1 : H_1 \cap H_2]$, und ist $\leqslant |G/H_2| = [G : H_2]$, woraus (a) folgt.

   (b) Mit Lagrange und (a) folgt

   $$[G : H_1 \cap H_2] = [G : H_1] \cdot [H_1 : H_1 \cap H_2] \leqslant [G : H_1] \cdot [G : H_2].$$

   (c) Wegen $H_1 \cap H_2' = (H_1 \cap H_2) \cap H_2'$ ist (c) genau die Aussage (a) für die Gruppen $H_1 \cap H_2 < H_2 > H_2'$ anstelle von $H_1 < G > H_2$.

2. Sei H eine echte Untergruppe einer endlichen Gruppe G.

   (a) Zeige, dass die Vereinigung aller Konjugierten von H nicht gleich G ist. (*Hinweis:* Zähle die Elemente in der Vereinigung $\bigcup_{g \in G} {}^g H$.)

   *(b) Gilt diese Aussage auch, wenn G nicht endlich ist?

   Lösung:

   (a) Sei $n := |G|$ und $m := |H|$ und $[G : H] = \ell$. Nach dem Satz von Lagrange gilt $n = m\ell$. Seien $g_1, g_2 \in G$, sodass $g_1 H = g_2 H$ ist. Dies impliziert $g_2^{-1} g_1 \in H$. Damit gilt

   $$g_2 H g_2^{-1} = g_2 g_2^{-1} g_1 H (g_2^{-1} g_1)^{-1} g_2^{-1} = g_1 H g_1^{-1}.$$

   Also gibt es höchstens $[G : H] = \ell$ verschiedene Konjugierte von H. Jede solche Konjugierte hat Kardinalität m und enthält das neutrale Element $e \in G$. Also enthält die Vereinigung aller Konjugierten höchstens $(m-1)\ell + 1 = n - \ell + 1$ Elemente. Da $G < H$ eine echte Untergruppe ist gilt $\ell > 1$ und somit $m\ell - \ell + 1 < n$. Also kann die Vereinigung aller Konjugierten nicht gleich G sein.

(b) Für unendliche Gruppen ist die Aussage im Allgemeinen falsch. Sei $n > 1$ und betrachte $G := \mathrm{GL}_n(\mathbb{C})$. Sei H die Untergruppe aller oberen Dreiecksmatrizen. Aus der linearen Algebra wissen wir, dass jedes Element von G ähnlich zu einer Matrix in Jordannormalform, also insbesondere zu einem Element von H ist. Da H eine echte Untergruppe von G ist, haben wir somit ein Gegenbeispiel gefunden.

*3. *(Lemma von Goursat).* Betrachte Gruppen G_1 und G_2 und eine Untergruppe H von $G_1 \times G_2$, so dass die beiden Projektionen $p_i : H \to G_i$ surjektiv sind. Zeige, dass es normale Untergruppen $N_1 \lhd G_1$ und $N_2 \lhd G_2$ gibt mit $(N_1 \times N_2) \lhd H$, so dass

$$H/(N_1 \times N_2) \;<\; (G_1 \times G_2)/(N_1 \times N_2) \;\cong\; (G_1/N_1) \times (G_2/N_2)$$

der Graph eines Isomorphismus $G_1/N_1 \xrightarrow{\sim} G_2/N_2$ ist.

Lösung: Write $(G_1 \times \{1\}) \cap H = N_1 \times \{1\}$ for some subset $N_1 \subset G_1$. As an intersection of subgroups $N_1 \times \{1\}$ is a subgroup of $G_1 \times \{1\}$. Applying the projection isomorphism $G_1 \times \{1\} \xrightarrow{\sim} G_1$ thus shows that N_1 is a subgroup of G_1.

Next consider any $g_1 \in G_1$. By the surjectivity of p_1 there exists $g_2 \in G_2$ with $h := (g_1, g_2) \in H$. The calculation

$$\begin{aligned}
{}^{g_1}N_1 \times \{1\} &= {}^{g_1}N_1 \times {}^{g_2}\{1\} \\
&= {}^{(g_1,g_2)}(N_1 \times \{1\}) \\
&= {}^{(g_1,g_2)}(G_1 \times \{1\}) \cap {}^{(g_1,g_2)}H \\
&= ({}^{g_1}G_1 \times {}^{g_2}\{1\}) \cap {}^{h}H \;= \\
&= (G_1 \times \{1\}) \cap H \\
&= N_1 \times \{1\}
\end{aligned}$$

thus shows that ${}^{g_1}N_1 = N_1$. Varying g_1 shows that $N_1 \lhd G_1$.

An analogous argument shows that $(\{1\} \times G_2) \cap H = \{1\} \times N_2$ for some normal subgroup $N_2 \lhd G_2$.

Now $N_1 \times N_2$ is a normal subgroup of $G_1 \times G_2$, and by construction we have $N_1 \times N_2 = (N_1 \times \{1\}) \cdot (\{1\} \times N_2) \subset H \cdot H = H$. Under the evident identification $(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$ we can view $H/(N_1 \times N_2)$ as a subgroup of $(G_1/N_1) \times (G_2/N_2)$.

We claim that for every coset $g_1N_1 \in G_1/N_1$ there exists a unique coset $g_2N_2 \in G_2/N_2$ such that $(g_1N_1, g_2N_2) \in H/(N_1 \times N_2)$. Indeed, the conclusion is equivalent to $(g_1, g_2) \in H$. The existence thus follows from the surjectivity of p_1. For any second coset $g_2'N_2 \in G_2/N_2$ with $(g_1, g_2') \in H$ the element $(g_1, g_2)^{-1}(g_1, g_2') = (1, g_2^{-1}g_2')$ lies in H and hence in $(\{1\} \times G_2) \cap H = \{1\} \times N_2$. Thus $g_2^{-1}g_2' \in N_2$, and so $g_2N_2 = g_2'N_2$, proving the uniqueness part of the claim.

The same argument on the other side shows that for every coset $g_2N_2 \in G_2/N_2$ there exists a unique coset $g_1N_1 \in G_1/N_1$ such that $(g_1N_1, g_2N_2) \in H/(N_1 \times N_2)$.

Together with the previous claim this implies that $H/(N_1 \times N_2)$ is the graph of a bijective map $\varphi\colon G_1/N_1 \to G_2/N_2$, namely sending g_1N_1 to g_2N_2 for any $g_2 \in G_2$ with $(g_1, g_2) \in H$. The two projection maps p_1 and p_2 in the commutative diagram

$$\begin{array}{ccccc} & & \dfrac{H}{N_1 \times N_2} & & \\ & \overset{p_1}{\swarrow} & \downarrow & \overset{p_2}{\searrow} & \\ \dfrac{G_1}{N_1} & \longleftarrow & \dfrac{G_1 \times G_2}{N_1 \times N_2} & \longrightarrow & \dfrac{G_2}{N_2} \end{array}$$

are therefore bijective. Since they are also group homomorphisms, they are isomorphisms, and hence so is $\varphi = p_2 \circ p_1^{-1}$, as desired.

4. Sei H eine Untergruppe einer Gruppe G und betrachte die Abbildung

$$\sigma\colon H \times G \to G,\ (h, g) \mapsto hg.$$

(a) Zeige, dass σ eine Linksoperation ist.

(b) Bestimme die Bahnen von σ.

(c) Wann ist die Operation σ transitiv, frei, treu, beziehungsweise trivial? Welches sind ihre Fixpunkte?

Lösung:

(a) Für alle $h, h' \in H$ und $g \in G$ gilt

$$\begin{aligned} \sigma(1_H, g) &= 1_H g = 1_G g = g \qquad \text{und} \\ \sigma(h, \sigma(h', g)) &= h(h'g) = (hh')g = \sigma(hh', g). \end{aligned}$$

Daher ist σ eine Linksoperation.

(b) Die Bahnen von σ sind genau die Teilmengen der Form $\{hg \mid h \in H\} = Hg$ für alle $g \in G$, das heisst, genau die Rechtsnebenklassen von H.

(c) Eine Operation heisst transitiv, wenn es genau eine Bahn gibt. In unserem Fall bedeutet dies, dass die triviale Nebenklasse $H1_G$ gleich G ist, also dass $H = G$ ist.

Eine Operation heisst frei, wenn kein nichttriviales Gruppenelement einen Fixpunkt hat. In unserem Fall ist $hg = g$ stets äquivalent zu $h = 1$; also ist die Operation immer frei.

Eine Operation heisst treu, wenn kein nichttriviales Gruppenelement alle Punkte festlässt. In unserem Fall lässt kein nichttriviales Element von H den Punkt $1_G \in G$ fest; also ist die Operation immer treu.

Eine Operation heisst trivial, wenn jedes Gruppenelement jeden Punkt festlässt. In unserem Fall bedeutet dies die Gleichung $hg = g$ für alle $h \in H$. Diese Gleichung ist äquivalent zu $h = 1$; somit ist die Operation genau dann trivial, wenn $H = 1$ ist.

Schliesslich ist ein Fixpunkt einer Operation ein Element, das von jedem Gruppenelement festgehalten wird. In unserem Fall bedeutet dies ein $g \in G$ mit $hg = g$ für alle $h \in H$. Dies ist wieder äquivalent zu $h = 1$ für alle $h \in H$, also zu $H = 1$. Somit ist die Fixpunktmenge gleich G im Fall $H = 1$, beziehungsweise leer im Fall $H \neq 1$.

5. Für eine natürliche Zahl n sei X die Menge aller Elemente der Ordnung 2 von S_n, auf der die S_n durch Konjugation operiert.

   (a) Bestimme die Anzahl und Längen der Bahnen dieser Operation.

   (b) Wann ist die Operation transitiv, frei, treu, beziehungsweise trivial? Welches sind ihre Fixpunkte?

   Lösung:

   (a) Betrachte ein Element $\sigma \in S_n$ der Ordnung 2. Dann ist die Kardinalität jeder Bahn von $\langle\sigma\rangle$ auf der Menge $\{1, \ldots, n\}$ ein Teiler von $|\langle\sigma\rangle| = 2$. Da ausserdem $\sigma \neq \mathrm{id}$ ist, muss es eine Bahn der Länge > 1 geben. Die Anzahl k der Bahnen der Länge 2 erfüllt also die Bedingungen $k \geqslant 1$ und $2k \leqslant |\{1, \ldots, n\}| = n$. Nach Proposition 1.13.13 der Vorlesung bilden alle Elemente der Ordnung 2 mit demselben k eine Konjugationsklasse in S_n; mit anderen Worten eine Bahn der Operation von S_n auf X. Die Anzahl dieser Bahnen ist daher die Anzahl der ganzen Zahlen k mit $1 \leqslant k \leqslant n/2$ und somit gleich $\lfloor \frac{n}{2} \rfloor$.

   Sodann ist ein σ wie oben schon durch die Zerlegung der Menge $\{1, \ldots, n\}$ in Bahnen bestimmt, da jede Bahn der Länge 1 einen Fixpunkt enthält und die Elemente jeder Bahn der Länge 2 miteinander vertauscht werden. Die Anzahl der σ vom Typ k ist daher die Anzahl der ungeordneten Zerlegungen von $\{1, \ldots, n\}$ in k Teilmengen der Länge 2 und $n - 2k$ Teilmengen der Länge 1. Die Auswahl der Bahnen der Länge 1 entspricht der Wahl einer Teilmenge der Ordnung $n - 2k$, wofür die Anzahl durch den Binomialkoeffizienten $\binom{n}{n-2k}$ gegeben ist. Wir müssen dies multiplizieren mit der Anzahl A_k der ungeordneten Zerlegungen einer Menge mit $2k$ Elementen in k ungeordnete Paare. Ohne Beschränkung der Allgemeinheit können wir diese Menge mit $\{1, \ldots, 2k\}$ identifizieren. Im Fall $k = 1$ ist offenbar $A_1 = 1$. Im Fall $k > 1$ muss das Element 1 mit einem beliebigen anderen Element gepaart sein. Für dieses andere Element gibt es genau $2k - 1$ Möglichkeiten. Für die Zerlegung der übrigen $2k - 2$ Elemente in Paare verbleiben dann genau A_{k-1} Möglichkeiten. Für $k > 1$ gilt also die Rekursionsformel $A_k = (2k - 1) \cdot A_{k-1}$.

Insgesamt ergibt sich dadurch

$$A_k \;=\; (2k-1)\cdot(2k-3)\cdots 3\cdot 1 \;=\; \frac{(2k)\cdot(2k-1)\cdots 2\cdot 1}{(2k)\cdot(2k-2)\cdots 4\cdot 2} \;=\; \frac{(2k)!}{2^k k!}.$$

Die gesuchte Länge ist daher

$$\binom{n}{n-2k}\cdot\frac{(2k)!}{2^k k!} \;=\; \frac{n!}{(n-2k)!(2k)!}\cdot\frac{(2k)!}{2^k k!} \;=\; \frac{n!}{(n-2k)!2^k k!}.$$

(b) Im Fall $n \leqslant 1$ ist $X = \varnothing$ und $S_n = 1$, also ist die Operation dann trivial und frei und treu, aber nicht transitiv und besitzt keine Fixpunkte. Im Fall $n = 2$ ist $|X| = 1 < 2 = |S_2|$, also ist die Operation dann trivial und transitiv, aber weder frei noch treu; ausserdem ist das einzige Element $(1\ 2) \in X$ ein Fixpunkt. Im Fall $n = 3$ besteht X aus einer einzigen Bahn der Länge $3 < 6 = |S_3|$, also ist die Operation transitiv, aber weder trivial noch frei, und sie hat keine Fixpunkte. Im Fall $n \geqslant 4$ hat die Operation mindestens zwei Bahnen, und nach (a) hat jede Bahn Länge > 1; darum ist die Operation weder transitiv noch trivial, und sie hat keine Fixpunkte. Da ausserdem jede Bahn eine Länge $< n! = |S_n|$ hat, ist die Operation auch nicht frei.

Schliesslich betrachte eine Permutation $\tau \in S_n$, die auf X trivial operiert. Dann fixiert τ insbesondere jeden 2-Zykel σ und kommutiert daher mit σ. Da alle 2-Zykel die S_n erzeugen, kommutiert τ also mit ganz S_n und liegt daher im Zentrum von S_n. Für $n \geqslant 3$ wissen wir aber, dass das Zentrum von S_n trivial ist. Darum ist die gegebene Operation für jedes $n \geqslant 3$ treu.

6. Für welche positiven ganzen Zahlen k, ℓ, m, n enthält die symmetrische Gruppe S_n einen k-Zykel und einen ℓ-Zykel, deren Produkt ein m-Zykel ist?

Lösung: Für beliebige $\rho, \sigma, \tau \in S_n$ gilt

$$\rho\sigma = \tau \Leftrightarrow \rho = \tau\sigma^{-1} \Leftrightarrow \tau^{-1}\rho = \sigma^{-1} \Leftrightarrow \tau^{-1} = \sigma^{-1}\rho^{-1} \Leftrightarrow \sigma\tau^{-1} = \rho^{-1} \Leftrightarrow \sigma = \rho^{-1}\tau.$$

Weiter ist ρ ein k-Zykel genau dann, wenn ρ^{-1} einer ist, und σ ist ein ℓ-Zykel genau dann, wenn σ^{-1} einer ist, und τ ist ein m-Zykel genau dann, wenn τ^{-1} einer ist. Die Antwort ist daher invariant unter beliebiger Vertauschung von k, ℓ, m.

Wir sammeln zuerst einige notwendige Bedingungen. Damit die S_n überhaupt einen k-Zykel enthält, muss $k \leqslant n$ sein. Eine notwendige Bedingung ist daher $k, \ell, m \leqslant n$. Sodann hat jeder k-Zykel das Signum $(-1)^{k-1}$. Eine weitere notwendige Bedingung ist daher $(-1)^{k-1}\cdot(-1)^{\ell-1} = (-1)^{m-1}$, das heisst $k+\ell \equiv m+1$ modulo (2). Weiter besitzt jeder k-Zykel $\rho \in S_n$ genau $n-k$ Fixpunkte in $\{1, \ldots, n\}$, und jeder ℓ-Zykel $\sigma \in S_n$ genau $n-\ell$ Fixpunkte. Der Durchschnitt dieser beiden Fixpunktmengen besteht dann aus Fixpunkten von $\rho\sigma$ und hat Kardinalität $\geqslant (n-k)+(n-\ell)-n = n-k-\ell$. Ist $\rho\sigma$ ein m-Zykel, so hat dieser aber genau

$n-m$ Fixpunkte, somit muss $n-k-\ell \leqslant n-m$ sein, also $m \leqslant k+\ell$. Aus Symmetriegründen gilt dann auch $k \leqslant \ell+m$ und $\ell \leqslant m+k$. Nach etwaiger Vertauschung können wir schliesslich $k, \ell \leqslant m$ annehmen. Die bisher gefundenen notwendigen Bedingungen sind dann äquivalent zu

$$1 \leqslant k, \ell \leqslant m \leqslant n \quad \text{und} \quad k+\ell \not\equiv m \bmod (2) \quad \text{und} \quad m \leqslant k+\ell.$$

Nun zeigen wir, dass diese Bedingungen hinreichend sind, und zwar durch Induktion über $k+\ell+m$. Im Fall $k=1$ implizieren die Bedingungen $\ell \equiv m \bmod (2)$ und $\ell \leqslant m \leqslant 1+\ell$ und damit $\ell = m$. Dann bilden der 1-Zykel $\rho = (1)$ und jeder m-Zykel σ eine Lösung. Das Entsprechende gilt im Fall $\ell = 1$.

Sodann betrachten wir den Fall $1 < k, \ell \leqslant m$ mit $k < m$. Dann erfüllen k und $\ell' := \ell - 1$ und $m' := m-1$ die Bedingungen

$$1 \leqslant k, \ell' \leqslant m' < n \quad \text{und} \quad k+\ell' \not\equiv m' \bmod (2) \quad \text{und} \quad m' \leqslant k+\ell'.$$

Nach der Induktionsvoraussetzung existieren daher ein k-Zykel $\rho \in S_{m'}$ und ein ℓ'-Zykel $\sigma' \in S_{m'}$, so dass $\rho\sigma'$ ein m'-Zykel ist. Wir erweitern diese Permutationen zu Elementen von S_n, indem wir sie trivial auf $\{m, m+1, \ldots, n\}$ operieren lassen. Nun wählen wir einen Index $1 \leqslant i \leqslant m'$, so dass $\sigma' i \neq i$ ist im Fall $\sigma' \neq \mathrm{id}$. Mit $\pi := (i\ m)$ ist dann $\sigma := \sigma'\pi$ in jedem Fall ein Zykel der Länge $\ell'+1 = \ell$, da σ' ein ℓ'-Zykel ist, der die Ziffer m nicht bewegt. Da $\rho\sigma'$ ein m'-Zykel in $S_{m'}$ ist, gilt auch $\tau\sigma' i \neq i$, und aus dem gleichen Grund ist folglich $\rho\sigma = \rho\sigma'\pi$ ein Zykel der Länge $m'+1 = m$. Damit haben wir eine Lösung gefunden.

Das entsprechende Argument geht im Fall $1 < k, \ell \leqslant m$ mit $\ell < m$ nach Vertauschung von k und ℓ.

Schliesslich verbleibt der Fall $1 < k = \ell = m$. In diesem Fall folgt aus $k+\ell \not\equiv m \bmod (2)$, dass k ungerade ist. Betrachte dann einen beliebigen k-Zykel $\rho \in S_n$ und setze $\sigma := \rho$. Da k ungerade ist, ist dann auch $\rho\sigma = \rho^2$ ein k-Zykel. Somit haben wir auch in diesem Fall eine Lösung gefunden und sind fertig.

7. Beschreibe die Ringe

   (a) $(\mathbb{Z}/15\mathbb{Z})[X]/(2X-4)$.

   (b) $(\mathbb{Z}/12\mathbb{Z})[X]/(2X-1)$.

   (c) $(\mathbb{Z}/6\mathbb{Z})[X]/(3X^2+3X+1)$.

   Lösung:

   (a) Wegen $2 \cdot 8 \equiv 1 \bmod (15)$ ist 2 eine Einheit in $\mathbb{Z}/15\mathbb{Z}$. Somit ist der Ring gleich

   $$(\mathbb{Z}/15\mathbb{Z})[X]/(X-2) \ \cong\ \mathbb{Z}[X]/(15, X-2) \ \cong\ (\mathbb{Z}[X]/(X-2))/(15).$$

Nun ist aber der Kern der Auswertungsabbildung $\mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}$ gleich $(X-2)$. Der Homomorphiesatz liefert daher einen Isomorphismus $\mathbb{Z}[X]/(X-2) \cong \mathbb{Z}$. Somit ist der fragliche Ring isomorph zu $\mathbb{Z}/(15) = \mathbb{Z}/15\mathbb{Z}$. Nach dem chinesischen Restsatz ist er auch isomorph zu $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

(b) Setze $R := (\mathbb{Z}/12\mathbb{Z})[X]/(2X-1)$. Wegen $(\mathbb{Z}/12\mathbb{Z})[X] \cong \mathbb{Z}[X]/(12\mathbb{Z}[X])$ gilt dann $R \cong \mathbb{Z}[X]/I$ für das Ideal $I := (12, 2X-1)$ von $\mathbb{Z}[X]$. Dieses Ideal

$$\begin{array}{lrcl} \text{enthält} & 6 & = & X \cdot 12 - 6 \cdot (2X-1) \\ \text{und daher} & 3 & = & X \cdot 6 - 3 \cdot (2X-1) \\ \text{sowie} & X-2 & = & -X \cdot 3 + 2 \cdot (2X-1); \end{array}$$

somit ist $J := (3, X-2) \subset I$. Umgekehrt sind $12 = 4 \cdot 3$ und $2X-1 = 3 + 2 \cdot (X-2)$ in J und daher $I \subset J$. Zusammen zeigt dies $I = J = (3, X-2)$. Wegen $\mathbb{Z}[X]/(3\mathbb{Z}[X]) \cong (\mathbb{Z}/3\mathbb{Z})[X] = \mathbb{F}_3[X]$ folgt nun

$$R \;\cong\; \mathbb{Z}[X]/(3, X-2) \;\cong\; \mathbb{F}_3[X]/(X-2) \;\cong\; \mathbb{F}_3.$$

(c) Setze $R := (\mathbb{Z}/6\mathbb{Z})[X]/(3X^2+3X+1)$. Wegen $(\mathbb{Z}/6\mathbb{Z})[X] \cong \mathbb{Z}[X]/(6\mathbb{Z}[X])$ gilt dann $R \cong \mathbb{Z}[X]/I$ für das Ideal $I := (6, 3X^2+3X+1)$ von $\mathbb{Z}[X]$. Dieses Ideal enthält das Element $2 \cdot (3X^2+3X+1) - (X^2+X) \cdot 6 = 2$ und ist daher gleich $(2, X^2+X+1)$. Somit ist

$$R \;\cong\; \mathbb{Z}[X]/I \;\cong\; (\mathbb{Z}/2\mathbb{Z})[X]/(X^2+X+1) \;=\; \mathbb{F}_2[X]/(X^2+X+1).$$

Nun ist X^2+X+1 ein Polynom vom Grad 2 ohne Nullstelle in $\mathbb{F}_2$. Somit ist es irreduzibel über $\mathbb{F}_2$. Da $\mathbb{F}_2[X]$ ein Hauptidealring ist, ist das Polynom also prim und der Faktorring ein Körper. Da die Restklassen von 1 und X eine Basis des Faktorrings über $\mathbb{F}_2$ bilden, hat dieser Körper die Dimension 2 über $\mathbb{F}_2$ und daher die Kardinalität 4. Somit ist R ein endlicher Körper der Ordnung 4.

*8. Sei R ein von Null verschiedener Ring und sei $a \in R \setminus \{0\}$. Wann ist der natürliche Homomorphismus $\varphi\colon R \to R[X]/(aX-1)$ injektiv?

Lösung: Betrachte ein Element $b \in R \setminus \{0\}$. Dann ist $\varphi(b) = 0$ genau dann, wenn b in dem Ideal $(aX-1)$ von $R[X]$ liegt. Dies bedeutet, dass ein Polynom $\sum_{i=0}^{n} c_i X^i$ mit $c_i \in R$ existiert, so dass

$$b \;=\; \sum_{i=0}^{n} c_i X^i (aX-1) \;=\; \sum_{i=0}^{n} a c_i X^{i+1} - \sum_{i=0}^{n} c_i X^i \;=\; a c_n X^{n+1} + \sum_{i=1}^{n} (a c_{i-1} - c_i) X^i - c_0$$

ist. Nach Koeffizientenvergleich ist dies äquivalent zu

$$a c_n = 0 \quad \text{und} \quad \forall\, 1 \leqslant i \leqslant n\colon a c_{i-1} = c_i \quad \text{und} \quad b = -c_0.$$

Insbesondere ist dann $c_n = -a^n b$, und die erste Gleichung impliziert $a \cdot (a^n b) = 0$. Falls also $\mathrm{Kern}(\varphi) \neq 0$ ist, ist a ein Nullteiler von R.

Sei umgekehrt a ein Nullteiler von R und wähle $b \in R$ mit $ab = 0$. Dann ist $b = -abX + b = -b(aX - 1)$ und damit $\varphi(b) = 0$. Wegen $a \neq 0$ ist dann ausserdem $b \neq 0$ und somit $\mathrm{Kern}(\varphi) \neq 0$.

Damit ist gezeigt, dass genau dann $\mathrm{Kern}(\varphi) \neq 0$ ist, wenn a ein Nullteiler von R ist. Somit ist φ genau dann injektiv, wenn a kein Nullteiler von R ist.

9. Finde für die folgenden reellen Zahlen x ein annullierendes Polynom von x über $\mathbb{Q}$ und folgere daraus eine einfachere Darstellung von x.

   (a) $x = \sqrt{4+\sqrt{7}} + \sqrt{4-\sqrt{7}}$.

   (b) $x = \sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}$.

   Lösung: (a) Wir rechnen mit der binomischen Formel

$$x^2 \;=\; (4+\sqrt{7}) + 2\sqrt{16-7} + (4-\sqrt{7}) \;=\; 4 + 2\cdot 3 + 4 \;=\; 14.$$

   Wegen $4 \pm \sqrt{7} > 0$ ist auch $x > 0$; somit folgt $x = \sqrt{14}$.

   (b) Wir rechnen mit der binomischen Formel

$$x^3 \;=\; (2+\sqrt{5}) + 3\sqrt[3]{4-5}\left(\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}\right) + (2-\sqrt{5}) \;=\; 4 - 3x.$$

   Also ist $X^3 + 3X - 4$ ein annullierendes Polynom für x. Dieses hat die Nullstelle 1 und die Faktorisierung $X^3+3X-4 = (X-1)(X^2+X+4)$. Die weiteren Nullstellen sind nicht reell, aber x schon; also gilt $x = 1$.

10. Sind die folgenden Körper isomorph?

    (a) $\mathbb{Q}[X]/(X^2-2)$ und $\mathbb{Q}[X]/(X^2+2)$;

    (b) $\mathbb{Q}[X]/(X^2+1)$ und $\mathbb{Q}[X]/(X^2+2)$;

    (c) $\mathbb{R}[X]/(X^2+1)$ und $\mathbb{R}[X]/(X^2+2)$;

    (d) $\mathbb{Q}[X]/(X^3-2)$ und $\mathbb{Q}[X]/(X^3+2)$.

    Lösung: (a) Wir können beide Körper in $\mathbb{C}$ einbetten via $\mathbb{Q}[X]/(X^2-2) \cong \mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}[X]/(X^2+2) \cong \mathbb{Q}(\sqrt{2}i)$. Ein Isomorphismus $\mathbb{Q}[X]/(X^2+2) \to \mathbb{Q}[X]/(X^2-2)$ entspricht damit einem Isomorphismus $\sigma\colon \mathbb{Q}(\sqrt{2}i) \to \mathbb{Q}(\sqrt{2})$. Dieser ist auf dem Primkörper $\mathbb{Q}$ die Identität; also ist $-2 = \sigma(-2) = \sigma((\sqrt{2}i)^2) = \sigma(\sqrt{2}i)^2$ ein Quadrat in $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$; Widerspruch. Somit sind die beiden Körper nicht isomorph.

Dasselbe Argument weniger formal: Das Polynom X^2-2 hat eine reelle Nullstelle, daher lässt sich der Körper $\mathbb{Q}[X]/(X^2-2)$ nach $\mathbb{R}$ einbetten. Das Polynom X^2+2 hat keine reelle Nullstelle, daher lässt sich der Körper $\mathbb{Q}[X]/(X^2+2)$ nicht nach $\mathbb{R}$ einbetten. Also können die beiden Körper nicht isomorph sein.

(b) Wie in (a) können wir $\mathbb{Q}[X]/(X^2+1) \cong \mathbb{Q}(i)$ und $\mathbb{Q}[X]/(X^2+2) \cong \mathbb{Q}(\sqrt{2}i)$ mit Unterkörpern von $\mathbb{C}$ identifizieren. Ihr Kompositum ist dann $\mathbb{Q}(\sqrt{2},i)$. Dieses hat den Unterkörper $\mathbb{Q}(\sqrt{2})$ vom Grad 2 über $\mathbb{Q}$, der in $\mathbb{R}$ enthalten ist und daher das Element i nicht enthält. Darum ist $[\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}(\sqrt{2})] = 2$ und somit $[\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}] = 4$. Wegen $[\mathbb{Q}(i)/\mathbb{Q}] = [\mathbb{Q}(\sqrt{2}i)/\mathbb{Q}] = 2$ sind nun aber beide Körper normal über $\mathbb{Q}$. Wäre also $\mathbb{Q}(i) \cong \mathbb{Q}(\sqrt{2}i)$, so wäre schon $\sqrt{2}i \in \mathbb{Q}(i)$ und daher $\mathbb{Q}(\sqrt{2},i) = \mathbb{Q}(i)$ vom Grad 2 über $\mathbb{Q}$; Widerspruch.

Aliter: Wie in (a) gilt für jeden Isomorphismus $\sigma\colon \mathbb{Q}(\sqrt{2}i) \to \mathbb{Q}(i)$ die Gleichung $\sigma(\sqrt{2}i)^2 = -2$. Wir zeigen durch direkte Rechnung, dass dies in $\mathbb{Q}(i)$ nicht möglich ist. Sei nämlich $(a+ib)^2 = -2$ mit $a,b \in \mathbb{Q}$. Dann ist $a^2 - b^2 + 2abi = -2$, also $a^2 - b^2 = -2$ und $2ab = 0$. Die erste Gleichung impliziert $b \neq 0$, was mit der zweiten $a = 0$ impliziert. In die erste Gleichung eingesetzt folgt daraus $b^2 = 2$. Aber in $\mathbb{Q}$ gibt es keine Quadratwurzel aus 2; Widerspruch.

(c) Wegen $\sqrt{2} \in \mathbb{R}$ induziert die Substitution $X \mapsto X/\sqrt{2}$ einen Isomorphismus.

(d) Ja, via der von $X \mapsto -X$ induzierten Abbildung.

Aliter: $\mathbb{Q}[X]/(X^3-2) \cong \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(-\sqrt[3]{2}) \cong \mathbb{Q}[X]/(X^3+2)$.

11. Betrachte die reellen Zahlen $\alpha := \sqrt{2}$ und $\beta := \sqrt{3}$ und setze $\gamma := \alpha + \beta$. Gilt $\mathbb{Q}[\alpha,\beta] = \mathbb{Q}[\gamma]$ als Unterringe von $\mathbb{R}$? Gilt $\mathbb{Z}[\alpha,\beta] = \mathbb{Z}[\gamma]$?

Lösung: Zur Vorbereitung berechnen wir $\gamma^2 = 5+2\sqrt{6}$ und daraus $\gamma^4 = 49 + 20\sqrt{6}$ $= 10\gamma^2 - 1$, sowie $\gamma^3 = 11\sqrt{2} + 9\sqrt{3}$. Letzteres impliziert $\alpha = (\gamma^3 - 9\gamma)/2 \in \mathbb{Q}[\gamma]$, und daraus folgt auch $\beta = \gamma - \alpha \in \mathbb{Q}[\gamma]$. Also gilt $\mathbb{Q}[\alpha,\beta] \subset \mathbb{Q}[\gamma] \subset \mathbb{Q}[\alpha,\beta]$ und somit $\mathbb{Q}[\gamma] = \mathbb{Q}[\alpha,\beta]$.

Sodann ist $\alpha \notin \mathbb{Q}$, aber $\alpha^2 = 2 \in \mathbb{Q}$; somit ist $\mathbb{Q}[\alpha]$ eine quadratische Körpererweiterung von $\mathbb{Q}$ mit der Basis $1,\alpha$. Wäre $\beta \in \mathbb{Q}[\alpha]$, so gäbe es also $a,b \in \mathbb{Q}$ mit $a + b\sqrt{2} = \sqrt{3}$. Quadrieren lieferte dann die Gleichung $a^2 + 2ab\sqrt{2} + b^2 = 3$, und nach Koeffizientenvergleich hätten wir $2ab = 0$. Dann wäre aber $a = 0$ und $b^2 = 3$, oder $b = 0$ und $a^2 = 3$, was beides in $\mathbb{Q}$ nicht möglich ist. Somit ist $\beta \notin \mathbb{Q}[\alpha]$. Wegen $\beta^2 = 3 \in \mathbb{Q}[\alpha]$ ist daher $\mathbb{Q}[\alpha,\beta]$ eine quadratische Körpererweiterung von $\mathbb{Q}[\alpha]$. Aus der Multiplikativität der Körpergrade folgt nun $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha,\beta] = 2\cdot 2 = 4$.

Wegen $\mathbb{Q}[\gamma] = \mathbb{Q}[\alpha,\beta]$ bilden die Elemente $1,\gamma,\gamma^2,\gamma^3$ deshalb eine Basis von $\mathbb{Q}[\gamma]$ über $\mathbb{Q}$. Insbesondere sind sie $\mathbb{Z}$-linear unabhängig. Aus $\gamma^4 = 10\gamma^2 - 1$ folgt nun, dass die additive Untergruppe $\mathbb{Z}\oplus\mathbb{Z}\gamma\oplus\mathbb{Z}\gamma^2\oplus\mathbb{Z}\gamma^3$ bereits ein Unterring und damit gleich $\mathbb{Z}[\gamma]$ ist. Wegen $\gamma = \alpha + \beta$ haben wir dabei $\mathbb{Z}[\gamma] \subset \mathbb{Z}[\alpha,\beta]$. Dagegen ist $\alpha = (\gamma^3 - 9\gamma)/2 = 0\cdot 1 - \frac{9}{2}\cdot\gamma + 0\cdot\gamma^2 + \frac{1}{2}\cdot\gamma^3$ die einzige $\mathbb{Q}$-Linearkombination von

$1, \gamma, \gamma^2, \gamma^3$ mit Wert α. Somit ist α keine $\mathbb{Z}$-Linearkombination dieser Elemente und damit nicht in $\mathbb{Z}[\gamma]$. Also ist $\mathbb{Z}[\gamma] \subsetneq \mathbb{Z}[\alpha, \beta]$.

12. Sei L/K eine endliche Körpererweiterung und sei $f \in K[X]$ irreduzibel.

    (a) Zeige: Sind $\deg(f)$ und $[L/K]$ teilerfremd, so ist f irreduzibel über L.

    (b) Gib Beispiele von irreduziblen Polynomen in $K[X]$ an, deren Grad nicht teilerfremd zu $[L/K]$ ist und die über L reduzibel sind.

    Lösung: (a) Nach Multiplikation mit einem konstanten Faktor können wir f als normiert annehmen. Sei g ein normierter irreduzibler Faktor von f in $L[X]$. Dann ist $M := L[X]/(g)$ eine Körpererweiterung von L, in der g die Nullstelle $a := X + (g)$ hat. Ausserdem ist $M = L(a)$ und g ist das Minimalpolynom von a über L. Sodann folgt aus $g(a) = 0$ auch $f(a) = 0$, und da f normiert und irreduzibel in $K[X]$ ist, ist es das Minimalpolynom von a über K. Für den Zwischenkörper $K(a) \subset M$ gilt daher $[K(a)/K] = \deg(f)$. Die Multiplikativität der Körpergrade impliziert nun

    $$[L(a)/L]\cdot[L/K] \;=\; [L(a)/K] \;=\; [L(a)/K(a)]\cdot[K(a)/K] \;=\; [L(a)/K(a)]\cdot\deg(f).$$

    Da $[L/K]$ und $\deg(f)$ teilerfremd sind, ist also $[L/K]$ ein Teiler von $[L(a)/K(a)]$. Andererseits gilt immer $[L(a)/K(a)] \leqslant [L/K]$, und deshalb hier Gleichheit. Insgesamt folgt daraus $[L(a)/L] = \deg(f)$. Da aber g das Minimalpolynom von a über L ist, ist $[L(a)/L] = \deg(g)$. Somit ist $\deg(g) = \deg(f)$ und amit $g = f$. Also ist f irreduzibel über L.

    (b) Für jedes $a \in L \smallsetminus K$ sei f das Minimalpolynom von a über K. Dann ist $f \in K[X]$ irreduzibel vom Grad > 1, hat aber die Nullstelle $a \in L$ und ist daher reduzibel über L.

13. Entscheide, ob man den Winkel $\arccos(11/16)$ mit Zirkel und Lineal dritteln kann.

    Lösung: Wir setzen $\alpha := \arccos\frac{11}{16}$ und $a := \cos\frac{\alpha}{3}$. Aus der Vorlesung wissen wir, dass ein Winkel genau dann konstruierbar ist, wenn sein Cosinus (oder äquivalenterweise sein Sinus) als Länge konstruierbar ist. Daher lässt sich der Winkel α genau dann dritteln, wenn a aus $\cos\alpha = 11/16$ konstruierbar ist.

    Die allgemeine Formel $\cos x = 4\cos^3\frac{x}{3} - 3\cos\frac{x}{3}$ ergibt

    $$\frac{11}{16} \;=\; \cos\alpha \;=\; 4a^3 - 3a.$$

    Folglich ist

    $$f(X) = 64X^3 - 48X - 11$$

    ein annullierendes Polynom von a. Die Substitution $Y = 4X$vereinfacht f zu dem Polynom $Y^3 - 12Y - 11$, für das man leicht sieht, dass es die Nullstelle -1 hat und

daher in $\mathbb{Q}[X]$ in Faktoren vom Grad $\leqslant 2$ zerfällt. Die Nullstelle $4a$ liegt somit in einer quadratischen Erweiterung von $\mathbb{Q}$ und ist konstruierbar, also gilt das auch für a. Somit lässt sich der Winkel α dritteln.

Genauer finden wir

$$Y^3 - 12Y - 11 = (Y + 1)(Y^2 - Y - 11).$$

Die Nullstellen dieses Polynoms sind $Y = -1, \frac{1\pm\sqrt{45}}{2}$. Folglich hat f die Nullstellen $-\frac{1}{4}, \frac{1\pm\sqrt{45}}{8}$. Wegen $0 < \frac{\alpha}{3} < \pi/2$ ist a positiv, daher gilt $a = \frac{1+\sqrt{45}}{8}$.

14. Sei R ein faktorieller Ring und I das von einer Teilmenge $A \subset R$ erzeugte Ideal. Was kann man sagen über die Menge aller Hauptideale, die I enthalten?

Lösung: Nach Definition ist I das eindeutige kleinste Ideal, welches A umfasst. Für ein beliebiges $b \in R$ gilt also $I \subset (b)$ genau dann, wenn $A \subset (b)$ ist. Wegen $(b) = \{xb \mid x \in R\}$ bedeutet dies, dass b jedes Element von A teilt, das heisst, ein gemeinsamer Teiler von A ist.

Ist $A \subset \{0\}$, so gilt dies für jedes $b \in R$. Andernfalls wähle ein $a \in A \smallsetminus \{0\}$ und schreibe $a = up_1 \cdots p_n$ mit $u \in R^\times$ und Primelementen $p_1, \ldots, p_n$. Die möglichen Teiler von a sind dann genau die Elemente der Form $v \prod_{i\in I} p_i$ für eine Einheit $v \in R^\times$ und eine Teilmenge $I \subset \{1, \ldots, n\}$. Insbesondere hat der grösste gemeinsame Teiler von je endlich vielen Elemente $a = a_1, \ldots, a_m \in A \smallsetminus \{0\}$ diese Form. Da es für die Teilmenge I nur endlich viele Möglichkeiten gibt, ist eine davon minimal. Für diese ist dann $v \prod_{i\in I} p_i$ ein grösster gemeinsamer Teiler von ganz A. Die möglichen b mit $I \subset (b)$ sind dann genau die Elemente der Form $v \prod_{i\in J} p_i$ für alle $v \in R^\times$ und allen Teilmengen $J \subset I$.

15. Für welche Ringe R ist der Polynomring $R[X]$ ein Hauptidealring?

Lösung: We already know that $R[X]$ is a principal ideal domain if R is a field. We claim that this is the only case. So assume that $R[X]$ is a principal ideal domain. Then $R[X]$ is in particular an integral domain; hence so is the subring R. From the natural isomorphism $R \xrightarrow{\sim} R[X]/(X)$ it follows that $R[X]/(X)$ is an integral domain, too. Thus the ideal (X) is a non-zero prime ideal. But in a principal ideal domain, every non-zero prime ideal is maximal. Thus (X) is a maximal ideal; hence $R[X]/(X) \cong R$ is a field.

16. Sei K ein Körper. Zeige, dass es unendliche viele irreduzible normierte Polynome in $K[X]$ gibt.

Lösung: Our proof is directly analogous to Euclid's proof that there are infinitely many prime numbers. We know that there exists a monic irreducible polynomial in $K[X]$ (for example $X - 1$). Take $n \geqslant 1$ distinct monic irreducible polynomials $p_1, \ldots, p_n$ in $K[X]$ and set

$$P := p_1 p_2 \cdots p_n + 1.$$

Then P is monic of degree > 0 and therefore possesses a monic irreducible factor p. We claim that p is distinct from each of the p_i. If $p = p_i$ for some $1 \leqslant i \leqslant n$, then it follows that $p|P$ and $p|(P-1) = \prod_i p_i$, from which it follows that $p|1$. Thus p is a unit, a contradiction. Hence for any finite set of monic irreducible elements in $K[X]$, we can find a monic irreducible not contained in that set. It follows that that set of monic irreducible polynomials in $K[X]$ is infinite.

*17. Sei $\mathcal{O}(\mathbb{C})$ der Ring aller holomorphen Funktionen $\mathbb{C} \to \mathbb{C}$.

(a) Welche Beziehung besteht zwischen $\mathcal{O}(\mathbb{C})$ und dem Ring $\mathcal{O}_p$ der Keime holomorpher Funktionen in einem Punkt $p \in \mathbb{C}$ aus Aufgabe 7 von Serie 12?

(b) Zeige, dass $\mathcal{O}(\mathbb{C})$ ein Integritätsbereich ist.

(c) Bestimme die Einheitengruppe von $\mathcal{O}(\mathbb{C})$.

(d) Bestimme alle irreduziblen Elemente von $\mathcal{O}(\mathbb{C})$.

(e) Beweise, dass alle diese schon Primelemente sind.

(f) Zeige, dass $\mathcal{O}(\mathbb{C})$ nicht faktoriell ist.

(g) Ist $\mathcal{O}(\mathbb{C})$ noethersch? (Siehe Satz 4.4.3 der Vorlesung.)

(h) Beschreibe den Quotientenkörper von $\mathcal{O}(\mathbb{C})$ mit Hilfe von meromorphen Funktionen. (*Hinweis*: Weierstrass'scher Produktsatz.)

Lösung: Zur Vorbereitung erinnern wir uns an die *Nullstellenordnung* $\operatorname{ord}_p(f)$ einer in einer Umgebung von $p \in \mathbb{C}$ holomorphen Funktion f. Für $f \neq 0$ ist dies die eindeutige ganze Zahl $n \geqslant 0$, so dass f in einer Umgebung von p als Potenzreihe in $z-p$ darstellbar ist mit dem Anfangsterm $a(z-p)^n$ für ein $a \in \mathbb{C}^\times$. Ausserdem ist $\operatorname{ord}_p(0) = \infty$. Diese Ordnung erfüllt die grundlegende Gleichung

$$\operatorname{ord}_p(fg) \;=\; \operatorname{ord}_p(f) + \operatorname{ord}_p(g).$$

(a) Jede Funktion $f \in \mathcal{O}(\mathbb{C})$ definiert einen eindeutigen Keim bei p; genauer haben wir einen wohldefinierten Ringhomomorphismus $\mathcal{O}(\mathbb{C}) \to \mathcal{O}_p$, $f \mapsto [(f, \mathbb{C})]$. Da zwei ganze Funktionen schon dann übereinstimmen, wenn sie in einer beliebig kleinen Umgebung von p übereinstimmen, ist dieser Homomorphismus injektiv.

(b) In Aufgabe 7 von Serie 12 haben wir gesehen, dass $\mathcal{O}_p$ ein Integritätsbereich (und sogar ein Hauptidealring) ist. Nach (a) ist $\mathcal{O}(\mathbb{C})$ isomorph zu einem Unterring davon; also ist auch $\mathcal{O}(\mathbb{C})$ ein Integritätsbereich.

Aliter: Für $f, g \in \mathcal{O}(\mathbb{C}) \smallsetminus \{0\}$ sind $\operatorname{ord}_0(f)$, $\operatorname{ord}_0(g) < \infty$ und daher auch $\operatorname{ord}_0(fg) < \infty$, also $fg \neq 0$. Wegen $\mathcal{O}(\mathbb{C}) \neq 0$ ist es also ein Integritätsbereich.

(c) Sind $f, g \in \mathcal{O}(\mathbb{C})$ mit $fg = 1$, so hat f keine Nullstelle. Wenn umgekehrt $f \in \mathcal{O}(\mathbb{C})$ keine Nullstelle hat, so ist auch die reziproke Funktion $\frac{1}{f}$ überall holomorph, also eine Inverse zu f in $\mathcal{O}(\mathbb{C})$ und daher eine Einheit.

(d-e) Wir behaupten, dass die irreduziblen Elemente in $\mathcal{O}(\mathbb{C})$ genau die Funktionen f mit einer einzigen und einfachen Nullstelle p sind, und dass diese prim sind. Dies resultiert aus den folgenden drei Lemmas:

Lemma 1: Für jedes solche f und jedes $g \in \mathcal{O}(\mathbb{C})$ mit $\mathrm{ord}_p(g) \geqslant 1$ ist $f|g$.

Beweis: Nach Voraussetzung ist $f(z)$ durch eine überall konvergente Potenzreihe der Form $a(z-p)+$ (höhere Terme) darstellbar mit $a \in \mathbb{C}^\times$. Also ist $f(z) = (z-p)\cdot f_1(p)$ für eine holomorphe Funktion $f_1(z) = a+$(höhere Terme), und nach Voraussetzung hat diese keine Nullstelle mehr und ist nach (c) also eine Einheit. Sodann ist g durch eine Potenzreihe der Form $b(z-p)+$(höhere Terme) darstellbar mit $b \in \mathbb{C}$. Also ist $g(z) = (z-p)\cdot g_1(p)$ für eine holomorphe Funktion g_1. Daher ist $g = f \cdot (g_1/f_1)$ mit $g_1/f_1 \in \mathcal{O}(\mathbb{C})$, also $f|g$. □

Lemma 2: Jedes solche f ist prim.

Beweis: Nach der Vorbemerkung ist $f \neq 0$ und nach (c) keine Einheit. Seien $g, h \in \mathcal{O}(\mathbb{C})$ mit $f|gh$, also mit $fk = gh$ für ein $k \in \mathcal{O}(\mathbb{C})$. Dann gilt

$$1 + \mathrm{ord}_p(k) \;=\; \mathrm{ord}_p(fk) \;=\; \mathrm{ord}_p(gh) \;=\; \mathrm{ord}_p(g) + \mathrm{ord}_p(h).$$

Also ist $\mathrm{ord}_p(g) \geqslant 1$ oder $\mathrm{ord}_p(h) \geqslant 1$, und mit Lemma 1 folgt daraus $f|g$ oder $f|h$. □

Lemma 3: Jedes $g \in \mathcal{O}(\mathbb{C})$ mit mehr als einer Nullstelle oder einer mehrfachen Nullstelle ist reduzibel.

Beweis: Sei p eine Nullstelle von g. Nach Lemma 1 gilt dann $g(z) = (z-p)h$ für ein $h \in \mathcal{O}(\mathbb{C})$. Ist $q \neq p$ eine weitere Nullstelle von g, oder $q = p$ eine mehrfache Nullstelle von g, so ist q auch eine Nullstelle von h; also ist h keine Einheit. Somit ist $g(z) = (z-p)\cdot h(z)$ eine Zerlegung von g in Nichteinheiten; also ist g reduzibel. □

(f) Nach (c-e) hat jedes endliche Produkt von Einheiten und/oder Primelementen höchstens endlich viele Nullstellen. Eine Funktion mit unendlich vielen Nullstellen, wie zum Beispiel $\sin(z)$, ist daher kein solches Produkt. Somit ist $\mathcal{O}(\mathbb{C})$ nicht faktoriell.

(g) Für jede natürliche Zahl n ist $f_n(z) := \sin(z/2^n)$ eine Funktion in $\mathcal{O}(\mathbb{C})$ mit der Nullstellenmenge $2^n\pi\mathbb{Z}$. Wegen

$$f_n(z) \;=\; \sin(\tfrac{z}{2^n}) \;=\; 2\sin(\tfrac{z}{2^{n+1}})\cdot\cos(\tfrac{z}{2^{n+1}}) \;=\; 2\cos(\tfrac{z}{2^{n+1}})\cdot f_{n+1}(z)$$

gilt $f_{n+1}|f_n$. Dass die Nullstellenmenge von f_{n+1} echt in der Nullstellenmenge von f_n enthalten ist, bedeutet dagegen $f_n \nmid f_{n+1}$. Für die zugehörigen Hauptideale von $\mathcal{O}(\mathbb{C})$ gilt daher $(f_n) \subsetneqq (f_{n+1})$. Die unendliche strikt aufsteigende Idealfolge $(f_0) \subsetneqq (f_1) \subsetneqq \ldots$ zeigt nun, dass $\mathcal{O}(\mathbb{C})$ nicht noethersch ist.

Aliter: Wäre $\mathcal{O}(\mathbb{C})$ noethersch, so könnte man wie im Beweis von Satz 4.4.3 der Vorlesung zeigen, dass R faktoriell ist, im Widerspruch zu (f).

(h) Wir behaupten, dass der Quotientenkörper von $\mathcal{O}(\mathbb{C})$ natürlich isomorph zu dem Körper $\mathcal{M}(\mathbb{C})$ der meromorphen Funktionen auf $\mathbb{C}$ ist.

Zunächst ist jede Funktion $g \in \mathcal{O}(\mathbb{C}) \smallsetminus \{0\}$ invertierbar in $\mathcal{M}(\mathbb{C})$. Nach der universellen Eigenschaft des Quotientenkörpers haben wir also einen wohldefinierten Körperhomomorphismus

$$\mathrm{Quot}(\mathcal{O}(\mathbb{C})) \longrightarrow \mathcal{M}(\mathbb{C}), \quad \tfrac{f}{g} \mapsto \tfrac{f}{g}.$$

Es bleibt zu zeigen, dass dieser surjektiv ist. Da die Nullfunktion offenbar im Bild ist, müssen wir zeigen, dass jedes $h \in \mathcal{M}(\mathbb{C}) \smallsetminus \{0\}$ als Quotient zweier von Null verschiedener Funktionen in $\mathcal{O}(\mathbb{C})$ geschrieben werden kann. Sei dafür P die Menge aller Polstellen von h. Aus der Funktionentheorie wissen wir, dass dies eine diskrete Teilmenge von $\mathbb{C}$ ist. Für jedes $p \in P$ sei sodann $n_p := -\operatorname{ord}_p(h)$ die Polordnung von h bei p. Nach dem Weierstrass'schen Produktsatz existiert nun eine holomorphe Funktion $g \in \mathcal{O}(\mathbb{C})$, welche genau in den Punkten von P Nullstellen besitzt, und zwar der Ordnung $\operatorname{ord}_p(g) = n_p$ für alle $p \in P$. (Siehe zum Beispiel [Freitag, Busam: Funktionentheorie 1, Kap. IV.2.]) Betrachte dann die meromorphe Funktion $f := gh \in \mathcal{M}(\mathbb{C})$. Nach Konstruktion ist sie holomorph ausserhalb von P, und für jedes $p \in P$ ist $\operatorname{ord}_p(f) = \operatorname{ord}_p(g) + \operatorname{ord}_p(h) \geqslant 0$. Also hat f dort nur hebbare Singularitäten, ist also repräsentiert durch eine überall holomorphe Funktion in $\mathcal{O}(\mathbb{C})$. Somit ist $h = f/g$ mit $f, g \in \mathcal{O}(\mathbb{C})$, wie zu zeigen war.

18. Zerlege für beliebige ganze Zahlen $m, n \geqslant 1$ das Polynom $X^m - Y^n \in \mathbb{C}[X, Y]$ in irreduzible Faktoren.

Lösung: Schreibe $m = m'\ell$ und $n = n'\ell$ mit $\ell \in \mathbb{Z}^{\geqslant 1}$ und teilerfremden $m', n' \in \mathbb{Z}^{\geqslant 1}$. Dann ist

$$X^m - Y^n \;=\; (X^{m'})^\ell - (Y^{n'})^\ell \;=\; \prod_{\zeta \in \mathbb{C},\ \zeta^\ell = 1} \big(X^{m'} - \zeta Y^{n'}\big).$$

Wir behaupten, dass jeder Faktor auf der rechten Seite irreduzibel ist. Betrachte dafür einen in X normierten Faktor $g \in \mathbb{C}[X, Y]$ von $X^{m'} - \zeta Y^{n'}$ vom Grad $0 < k \leqslant m'$. Wähle $\xi \in \mathbb{C}$ mit $\xi^{m'} = \zeta$. Nach der Substitution $Y = Z^{m'}$ haben wir dann

$$X^{m'} - \zeta (Z^{m'})^{n'} \;=\; X^{m'} - (\xi Z^{n'})^{m'} \;=\; \prod_{\rho \in \mathbb{C},\ \rho^{m'} = 1} \big(X - \rho \xi Z^{n'}\big),$$

und $g(X, Z^{m'})$ ist ein Produkt von k dieser Faktoren. Dessen konstanter Koeffizient ist daher in $\mathbb{C}^\times \cdot (Z^{n'})^k$. Andererseits entsteht er durch die Substitution $Y = Z^{m'}$ aus einem Polynom in Y. Somit ist $Z^{n'k}$ ein Polynom in $Z^{m'}$. Wegen $0 < k \leqslant m'$ und $\mathrm{ggT}(m', n') = 1$ ist dies nur möglich mit $k = m'$. Also ist $X^{m'} - \zeta Y^{n'}$ irreduzibel in $\mathbb{C}[X, Y]$.

*19. Sei R ein faktorieller Ring. In der Vorlesung haben wir gezeigt, dass jeder Polynomring in endlich vielen Variablen über R ebenfalls faktoriell ist. Gilt dies auch für einen Polynomring in einer beliebig grossen unendlichen Menge von Variablen?

Lösung: Betrachte eine Menge I und unabhängige Variable X_i für alle $i \in I$. Für jede Teilmenge $J \subset I$ sei R_J der Polynomring über R in den Variablen X_i für $i \in J$. Dann ist R_I die Vereinigung der R_J für alle endlichen Teilmengen $J \subset I$.

Wegen $1 \neq 0$ in R gilt dies auch in R_I. Sodann betrachte $f, g \in R_I \smallsetminus \{0\}$. Wähle $J \subset I$ endlich mit $f, g \in R_J$. Da R_J ein Integritätsbereich ist, gilt dann $fg \neq 0$ in R_J und damit auch in R_I. Somit ist R_I ein Integritätsbereich. Gilt weiter $fg = 1$ in R_J, so gilt dies auch in R_I; also ist jede Einheit in R_J auch eine Einheit in R_I.

Sodann behaupten wir, dass jedes Primelement $p \in R_J$ auch ein Primelement in R_I ist. Dafür betrachte zuerst eine beliebige endliche Teilmenge $J' \subset I$ mit $J \subset J'$. Dann ist $R_{J'}$ ein Polynomring in endlich vielen Variablen über R_J. In §4.6 der Vorlesung haben wir gesehen, dass p dann auch ein Primelement in $R_{J'}$ ist. Insbesondere ist $p \neq 0$ und keine Einheit in $R_{J'}$. Wäre p eine Einheit in R_I, so gäbe es ein $q \in R_I$ mit $pq = 1$, und dieses q läge in einem solchen $R_{J'}$, also wäre p eine Einheit in $R_{J'}$: Widerspruch. Somit ist p keine Einheit in R_I. Betrachte nun $f, g \in R_I$ mit $p|fg$ in R_I. Dann existiert ein $h \in R_I$ mit $ph = fg$. Wähle die obige endliche Menge J' so, dass $f, g, h \in R_{J'}$ sind. Dann gilt $p|fg$ in $R_{J'}$, und da p ein Primelement von $R_{J'}$ ist, folgt $p|f$ oder $p|g$ in $R_{J'}$. Also existiert ein $k \in R_{J'}$ mit $pk = f$ oder $pk = g$. Diese Gleichung gilt dann auch in R_I; somit folgt $p|f$ oder $p|g$ in R_I. Damit ist gezeigt, dass p ein Primelement von R_I ist.

Betrachte schliesslich ein beliebiges $f \in R_I$. Wähle J mit $f \in R_J$ und eine Zerlegung $f = uf_1 \cdots f_r$ mit einer Einheit $u \in R_J^\times$ und Primelementen $f_1, \ldots, f_r \in R_J$. Nach den obigen Bemerkungen sind dann $u \in R_I^\times$ und $f_1, \ldots, f_r$ Primelemente in R_I. Somit ist R_I faktoriell.

20. Bestimme welche der folgenden Polynome irreduzibel sind.

(a) $X^3 + 9X + 6X - 3 \in \mathbb{Z}[X]$.

(b) $4X^3 - 15X^2 + 60X + 180 \in \mathbb{Q}[X]$.

(c) $X^3 + 3X^2 + 5X + 5 \in \mathbb{Q}[X]$

(d) $X^7 + 7X^6 + 5X^2 - X + 1 \in \mathbb{R}[X]$.

(e) $X^4 - X^2 - 2X + 3 \in \mathbb{Z}[X]$.

(f) $X^7 - X^6 + X^5 + 16X^4 + 17X^3 + 6X + 17 \in \mathbb{Z}[X]$.

Lösung: (a) Irreduzibel nach dem Eisensteinkriterium für $p = 3$, da normiert.

(b) Das Polynom ist normiert; nach dem Eisensteinkriterium für $p = 5$ ist es also irreduzibel in $\mathbb{Z}[X]$ und somit auch in $\mathbb{Q}[X]$.

(c) Die Reduktion modulo 3 ist $X^3 - X - 1$ und hat keine Nullstelle in $\mathbb{F}_3$. Da sie Grad 3 hat, ist sie somit irreduzibel. Da das ursprüngliche Polynom normiert ist, ist es daher selbst irreduzibel in $\mathbb{Z}[X]$ und damit auch in $\mathbb{Q}[X]$.

(d) Da $\mathbb{C}$ algebraisch abgeschlossen ist, zerfällt das Polynom über $\mathbb{C}$ in Linearfaktoren. Die Nullstellen in $\mathbb{Z} \smallsetminus \mathbb{R}$ kommen in Paaren komplex konjugierter Zahlen mit derselben Multiplizität. Da das Polynom ungeraden Grad hat, besitzt es daher eine Nullstelle in $\mathbb{R}$ und damit einen Linearfaktor in $\mathbb{R}[X]$. Da es nicht selbst linear ist, ist es reduzibel.

(e) Das Polynom ist normiert und besitzt die Zerlegungen in irreduzible Faktoren $(X^2 + X + 1)^2$ modulo (2), beziehungsweise $X(X^3 + 2X + 1)$ modulo (3). Diese implizieren, dass das Polynom keinen Faktor vom Grad 1, beziehungsweise 2 in $\mathbb{Z}[X]$ hat; also ist es irreduzibel. *Aliter:* Das Polynom ist schon irreduzibel modulo (7) und daher selbst irreduzibel.

(f) Das Polynom ist normiert. Seine irreduziblen Faktoren modulo (3) haben die Grade $3 + 3 + 1$ und modulo (5) die Grade $2 + 5$. Ist das Polynom reduzibel in $\mathbb{Z}[X]$, so kann es wegen letzterem nur eine Zerlegung in die Grade $2 + 5$ haben, was aber wegen ersterem nicht sein kann. Darum ist das Polynom irreduzibel.